Symantec AntiVirus™/Filtering for Domino™ for SPARC Solaris™ Implementation Guide

Symantec AntiVirus™/Filtering for Domino™ for SPARC Solaris™ Implementation Guide

Documentation version 3.0

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE

THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION AND DOCUMENTATION.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the quantity of the Software for which You have paid the applicable license fees after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of licensed copies of this Software are as follows:

YOU MAY:

A. use the Software in the manner described in the Software documentation and in accordance with the License Module. If the Software is part of an offering containing multiple Software titles, the aggregate number of copies You may use may not exceed the aggregate number of licenses indicated in the License Module, as calculated by any combination of licensed Software titles in such offering. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network or to protect a network such as at the gateway or on a mail server, provided that You have a license to the Software for each computer that can access the network;

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and

E. use the Software in accordance with any additional permitted uses set forth in Section 8, below.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

F. use the Software in any manner not authorized by this license; nor

G. use the Software in any manner that contradicts any additional restrictions set forth in Section 8, below.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which You have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit You to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT

OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE.

The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. The original of this Agreement has been written in English and English is the governing language of this Agreement. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

8. ADDITIONAL RESTRICTIONS FOR SPECIFIED SOFTWARE:

A. If the Software You have licensed is a specified Symantec AntiVirus™ for a third-party product or platform, You may use that specified Software with the corresponding product or platform only. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use Symantec AntiVirus Scan Engine.

B. If the Software you have licensed is Symantec AntiVirus for NetApp® Filer, the following additional use(s) and restriction(s) apply:

i)You may use the Software only with a NetApp Filer server;

ii)You may use the Software only with files accessed through a NetApp Filer; and

iii)You may not use the Software on a server that exceeds the specified capacity set forth in Your License Module.

C. If the Software you have licensed is Symantec AntiVirus for Web Servers, the following additional use(s) and restriction(s) apply:

i)You may use the Software only with files that are received from third parties through a Web server;

ii)You may use the Software only with files received from less than 10,000 unique third parties per month; and

iii)You may not charge or assess a fee for use of the Software for Your internal business.

D. If the Software You have licensed is Symantec Web Security, independent of version or operating platform designation, upon the expiration of Your right to acquire Content Updates, the filtering definitions corresponding with all previous Content Updates will be entirely deleted and will no longer be available for use with the Software. Upon the expiration of Your right to acquire Content Updates, access to updated virus definitions will no longer be available; however, You may continue to use virus definitions previously acquired.

E. If the Software You have licensed is Symantec AntiVirus Corporate Edition, You may not use the Software on or with devices on Your network running embedded operating systems specifically supporting network attached storage functionality without separately licensing a version of such Software specifically licensed for a specific type of network attached storage device under a License Module.

F. If the Software You have licensed is Symantec AntiVirus for EMC® Celerra™ File Server, You may use the Software only with EMC Celerra servers and only if You have a license to the Software for each Celerra AntiVirus Agent (CAVA) associated with each such server. You may not allow any computer to access the Software other than an EMC Celerra server.

NetApp is a registered trademark of Network Appliance, Inc. in the U.S. and other countries.

EMC and Celerra are trademarks or registered trademarks of EMC Corporation in the U.S. and other countries.

Contents

Chapter 1

Introducing Symantec AntiVirus/Filtering for Domino

This chapter includes the following topics:

About Symantec AntiVirus/Filtering for Domino

Symantec AntiVirus/Filtering for Domino is a complete, customizable, and scalable antivirus and filtering solution. It protects your Lotus Domino servers from viruses and destructive programs and lets you specify the actions to take, and notifications and alerts to issue, when a threat is detected. Additionally, Symantec AntiVirus/Filtering for Domino lets you filter email subject lines and message bodies for undesirable content, such as offensive language, confidential information, and spam email. The criteria that are used to identify threats are customizable. You can create and save multiple sets of criteria for use by Symantec AntiVirus/Filtering for Domino.

Symantec AntiVirus/Filtering for Domino is completely integrated into the Lotus Domino environment. It is comprised of the following Lotus databases:

- Settings (sav.nsf): Contains the protection and notification settings for your Lotus Domino servers. You configure protection and notification using this database.
- Log/Quarantine (savlog.nsf): Contains quarantined and backup documents, server messages, product version information, reports of virus incidents or content violations, scan summaries, and predefined statistical reports.
- Help (savhelp.nsf): Contains online help for Symantec AntiVirus/Filtering for Domino.

All scanning is configured and initiated from the Settings database (sav.nsf). All reports and virus dispositions are handled through the Log database (savlog.nsf). Information about the product and how to use it is provided in the Help database (savhelp.nsf). In addition, if you plan to replicate updated virus definitions, you must create a Definitions database (savdefs.nsf) in which to store the updated virus definitions.

Configuration capabilities

You can configure Symantec AntiVirus/Filtering for Domino to do any of the following:

- Eliminate viruses automatically on detection.
- Eliminate or filter email that contains unwanted content.
- Quarantine infected documents and email for administrator review.
- Delete infected items.

When viruses or content violations are detected, you can have Symantec AntiVirus/Filtering for Domino send email notifications to specified administrators, document or email authors, and intended email recipients.

How Symantec AntiVirus/Filtering for Domino works

Symantec AntiVirus/Filtering for Domino secures your Lotus Domino environment against virus attacks and unwanted content by protecting databases on Lotus Domino servers and monitoring email that is routed through the servers. Symantec AntiVirus/Filtering for Domino operation is transparent to users, with minimal performance degradation to the network.

Remember, however, that the Lotus Domino environment is only one avenue that a virus can use to penetrate your site. For a complete virus protection solution, make sure that the appropriate workstation or server version of Symantec AntiVirus is installed on every computer at your site as well.

About computer viruses, Trojan horses, and worms

A *virus* is a computer program written by an ill-intentioned programmer. When run, a virus attaches a copy of itself to another computer program or document. Whenever the infected program is run or the infected document is opened, the virus is activated and attaches itself to other programs and documents.

In addition to replicating, viruses are generally programmed to deliver payloads. Most viruses simply display a message on a trigger date. Some, however, are programmed to damage data by corrupting programs, deleting files, or reformatting disks.

The following classes of viruses pose the greatest threat in the Lotus Domino environment:

- Macro viruses: Infect word processing and spreadsheet documents (such as Microsoft Word or Excel documents)
- Program viruses: Infect executable files

Viruses spread as attachments or embedded OLE objects in Lotus Notes email and documents that are written to Lotus Notes databases on servers.

Trojan horses are malicious programs that are disguised as useful programs, such as utilities or games. An important distinction between Trojan horses and viruses is that Trojan horses do not replicate themselves. When you install and run a Trojan horse, it appears to be performing a helpful function, while it is actually damaging your computer's operating system.

Worms are programs that propagate from computer to computer, often by placing copies of themselves in each computer's memory. Worms usually exist inside of other files, such as Microsoft Word or Excel documents. A worm may replicate itself many times on one computer, which causes the computer to crash.

Symantec AntiVirus/Filtering for Domino detects and eliminates viruses, Trojan horses, and worms.

How viruses are detected

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. Once a virus is identified, information about the virus (a virus signature) is stored in a virus definitions file, which contains the necessary information to detect and eliminate the virus. When Symantec AntiVirus/Filtering for Domino scans for viruses, it is searching for these virus signatures.

To supplement detection of known viruses, Symantec AntiVirus/Filtering for Domino includes a Bloodhound technology. With this advanced heuristic technology, Symantec AntiVirus/Filtering for Domino can detect a high percentage of new or unknown viruses that have not yet been analyzed by antivirus researchers.

The Symantec AntiVirus/Filtering for Domino LiveUpdate feature keeps your virus protection current. Updated virus definitions files are provided by Symantec regularly. With LiveUpdate, Symantec AntiVirus/Filtering for Domino connects automatically to a Symantec site, determines if your files need updating, downloads the proper files, and installs them in the proper locations.

How unwanted content is filtered

In addition to Real Time, Scheduled, and Scan Now scans, the integration of content filtering into Symantec AntiVirus/Filtering for Domino enhances protection by blocking email and database writes based on content, and filtering email for spam messages in real time.

Using content filtering features, you can do the following:

- Search the subject lines or contents of email messages for offensive language, confidential information, and content with potential legal consequences.
- Identify spam email to delete, based on document attributes such as attachment size or extension, document sender, and Domino or Internet domain.
- Search for messages with particular subject lines.

To search for unwanted content, you create Content Filtering Rules. When the content or some attribute of a document violates a rule, Symantec AntiVirus/Filtering for Domino takes action according to the settings that you supplied for that rule.

You can set up as many content filters (rules) as needed. Each rule specifies the email category to search (subject line, sender, or attachment size, for example), and defines the condition that will trigger a content violation.

For example, you could set up a rule to filter email with attachments that exceed 3 MB in size. Symantec AntiVirus/Filtering for Domino would then catch any email messages with attachments that exceed 3 MB and, like other scans, would process the email according to your configuration settings. You can enable or disable content filtering at any time.

Chapter 2

Installing Symantec AntiVirus/Filtering for Domino

This chapter includes the following topics:

Installation overview

The Symantec AntiVirus/Filtering for Domino setup program creates a directory named Symantec that contains Symantec products (shared libraries and executable files). By default, the Symantec directory is installed to /opt, however, during install you can specify a different location. In addition, Symantec AntiVirus/Filtering for Domino also creates the following directories:

- .../Symantec/bin
  Symantec AntiVirus/Filtering for Domino engine
- <Domino server's default data directory>/sav
  Symantec AntiVirus/Filtering for Domino databases (sav.nsf, savlog.nsf, and savhelp.nsf)
- .../Symantec/virusdefs
  Virus definitions files that are specific for the operating system
- .../Symantec/LiveUpdate
  Technology to download virus definitions files and program updates

System requirements for Solaris SPARC

Root-level privileges are required to install or uninstall Symantec AntiVirus/Filtering for Domino for Solaris. The minimum system requirements listed in Table 1 and Table 2 must be met.

Table 1 Domino Server R5

Operating system	Solaris 2.6, 7, or 8
Lotus Domino	Domino Server R5 version 5.0.8 or later
Available disk space	200 MB

Table 2 Domino Server 6

Operating system	Solaris 8
Lotus Domino	Domino Server 6 version 6.0
Available disk space	200 MB

Installing Symantec AntiVirus/Filtering for Domino

Earlier versions of Norton AntiVirus for Lotus Notes/Domino should be uninstalled before installing Symantec AntiVirus/Filtering for Domino.

See "Uninstalling earlier versions of Norton AntiVirus for Lotus Notes" on page 20.

For Symantec AntiVirus/Filtering for Domino to function properly, the avdefs group must exist. This can be accomplished in two ways:

- The avdefs group exists on the computer on which the Domino server runs.
- The avdefs group is valid on the computer on which the Domino server runs.
  For example, the avdefs group is maintained on an NIS server and the computer on which the Domino server runs has access to those NIS controlled accounts.

The avdefs group can be created and populated at install time by the Symantec AntiVirus/Filtering for Domino installation script, or you can create the group and add Notes users manually before performing the Symantec AntiVirus/Filtering for Domino installation. The installation script will not complete if the avdefs group does not already exist or you do not allow the installation script to create the group itself.

Note: All Notes server user accounts (server user IDs) that are going to have Symantec AntiVirus/Filtering for Domino installed into their respective Notes partitions must be added as members of the avdefs group.

After installation, when Domino users have been added to the avdefs group, any terminal sessions launching Domino must be logged off and logged on again to ensure that the group membership and associated permissions are enabled. Failure to do this prevents Symantec AntiVirus/Filtering for Domino from locating virus definitions on startup, and, subsequently, not loading completely.

To install Symantec AntiVirus/Filtering for Domino

1. Shut down the Lotus Notes server.
2. Go to the CD-ROM directory (cd /cdrom).
3. Run the shellscript ./install from the Symantec AntiVirus/Filtering for Domino CD-ROM.
   If you have multiple Lotus Notes partitions on the same server, separate Symantec AntiVirus/Filtering for Domino databases are required for each

partition. Setup detects and lets you specify on which partitions to install Symantec AntiVirus/Filtering for Domino.

4. After the Symantec AntiVirus/Filtering for Domino install completes, restart the Lotus Notes server.

   When the Lotus Notes server is restarted, the Symantec AntiVirus/Filtering for Domino databases are created from templates and placed in the sav subdirectory of your default Data directory. A readme.txt file is placed in this directory as well.

5. Start the Lotus Notes client.
6. Select the workspace tab on which you want to place Symantec AntiVirus/Filtering for Domino.
7. On the File menu, click **Database** > **Open**.
8. Select the appropriate server. In the sav folder, open the SAV Settings database.

Install script options

The install shellscript can install Symantec AntiVirus/Filtering for Domino either interactively or non-interactively:

- Interactively: No command-line options are supplied.
- Non-interactively: The -p and -s options are specified on the command line.

Syntax

./install [-h] [-p <notespartition>] [-s <Symantec base directory>] [-d]

Options

The following command-line options are available:

-h	Displays the command-line syntax.
-p	Specifies the full path to the Notes partition on which to install Symantec AntiVirus/Filtering for Domino. Multiple Notes partitions, separated with commas, can be specified.
-s	Specifies the full path to the Symantec base directory that will contain all the Symantec AntiVirus/Filtering for Domino binary files. The -s option cannot be used on its own; it is used only in conjuction with the -p option.
-d	Specifies that the Symantec AntiVirus/Filtering for Domino installation process should use default settings. The -d option must be specified if the avdefs group does not yet exist or the install will fail.

The following example installs Symantec AntiVirus/Filtering for Domino to two Notes partitions in the default Symantec directory:

./install -p /notesdata1,/notesdata2 -d

Securing the databases

To secure your Symantec AntiVirus/Filtering for Domino databases after installation, perform the following tasks for both the sav.nsf and savlog.nsf databases:

- Modify the Access Control List to restrict access to antivirus or Lotus administrators only.
- Sign the databases with a Trusted ID from your organization to maintain the security of the Execution Control List of Notes clients that access the databases.

To modify the Access Control List

1. Right-click the Symantec AV/F (sav.nsf) icon, then click **Database** > **Access Control**.
2. Select users and grant them Manager access with Delete rights.

3 Repeat steps 1 and 2 for the Log database (savlog.nsf).

Note: Be sure to keep Manager access for the server group LocalDomainServers or Symantec AntiVirus/Filtering for Domino will not operate properly.

To maintain security for the Execution Control List of Notes clients

- Properly sign the Settings (sav.nsf) and Log (savlog.nsf) databases with a Trusted ID.

  For information on signing databases, search the Domino Administrator help database for the "tools - database - sign" topic.

Uninstalling earlier versions of Norton AntiVirus for Lotus Notes

Earlier versions of Norton AntiVirus for Lotus Notes/Domino should be uninstalled before installing Symantec AntiVirus/Filtering for Domino.

Uninstalling Norton AntiVirus version 2.1

Root-level privileges are required to uninstall Norton AntiVirus.

To uninstall Norton AntiVirus version 2.1

1. Stop the Domino server.
2. Switch to superuser or equivalent.
3. Change to the /opt/lotus/notes/symantec/uninstall/ directory.
4. Type the following at the command prompt:
   ./uninstallnav
5. Follow the prompts.
6. After the uninstall completes, exit superuser state and restart the Domino server.

Note: To verify that Norton AntiVirus is uninstalled, examine the server's notes.ini file. The line NSF_HOOKS=nhook should not be present and nntask should be removed from the ServerTasks line.

Uninstalling Norton AntiVirus version 2.5

Root-level privileges are required to uninstall Norton AntiVirus.

Backup files are not removed during the uninstall process. Norton AntiVirus for Lotus Notes makes a backup file of any existing file that gets written to or changed during the installation process. For example, the notes.ini file located in the .../<notesdata> directory is modified during the installation process. As a courtesy to administrators, a backup of the original notes.ini file is created. The backup file is called notes.ini.symbak and is not removed during the uninstall process.

To uninstall Norton AntiVirus version 2.5

1. Stop the Domino server.
2. Switch to superuser or equivalent.
3. Change to the .../symantec/NavNotes/uninstall directory.
4. Type the following at the command prompt:
   ./uninstallnav
5. Follow the prompts.

After the uninstall completes, you can manually remove backup files. Leaving these files, however, will not affect server performance. The following files may need to be removed manually.

- /etc/group.symbak
- /etc/liveupdate.conf.symbak
- /etc/Symantec.conf.symbak
- .../<notesdata>/notes.ini.symbak

Replicating the Settings and Log databases

The Settings database, sav.nsf, can be replicated to other Domino servers that are running Symantec AntiVirus/Filtering for Domino. The Symantec AntiVirus/Filtering for Domino server task, nntask, monitors sav.nsf for changes to the Symantec AntiVirus/Filtering for Domino settings through replication and reloads the settings on the local server. Symantec AntiVirus/Filtering for Domino settings can be distributed by manual or scheduled replication.

The following subset of settings in the Settings database are replicated between Domino servers:

- Real Time scanning settings
- Global AntiVirus options settings
- All Scheduled Scans
- Content Filtering Rules and options

The Log database, savlog.nsf, stores server messages, reports of virus incidents, and scan summaries. It also provides access to quarantined documents and documents that Symantec AntiVirus/Filtering for Domino backs up before eliminating viruses. Through replication, you can maintain a master Log that automatically includes virus incidents and statistics reports from other Domino servers that are running Symantec AntiVirus/Filtering for Domino.

Before Symantec AntiVirus/Filtering for Domino is installed

Use the following procedure to set up Settings and Log database replication if Symantec AntiVirus/Filtering for Domino is not yet installed.

To prepare for Settings and Log database replication

1. Select a server in your organization to be the master Symantec AntiVirus/Filtering for Domino server.
2. Install Symantec AntiVirus/Filtering for Domino on the server and start the Domino server on that computer.
3. Ensure that Notes administrators and LocalDomainServers are in the Access Control List of sav.nsf and savlog.nsf, with Manager access and Delete Documents enabled.

   The LocalDomainServers group should contain all of the servers to which you plan to replicate.
4. Before you install Symantec AntiVirus/Filtering for Domino on other servers, create replicas of the newly installed sav.nsf and savlog.nsf databases in the sav directory in the default data directory of the other Domino servers.
5. Install Symantec AntiVirus/Filtering for Domino on the other servers, but keep the already replicated sav.nsf and savlog.nsf databases.

   This is an option of the Symantec AntiVirus/Filtering for Domino setup program.

Any changes that are made to Symantec AntiVirus/Filtering for Domino settings on any of the Domino servers are distributed to the other replicas when a manual

or scheduled replication occurs. After replication, the new Symantec AntiVirus/Filtering for Domino settings are reloaded automatically.

Note: Replication conflicts can be avoided by permitting only the Notes administrator who is in charge of antivirus policy to edit the Symantec AntiVirus/Filtering for Domino settings on each of the Domino servers.

For the Log, initiate push replication from the Symantec AntiVirus/Filtering for Domino Log replicas to the master savlog.nsf. This centralizes the logging of virus incidents across the network.

After Symantec AntiVirus/Filtering for Domino is installed

Use the following procedure to set up Settings and Log database replication if Symantec AntiVirus/Filtering for Domino is already installed. You must stop the server task on a server on which Symantec AntiVirus/Filtering for Domino is already installed before replicating the databases.

To stop the Symantec AntiVirus/Filtering for Domino server task on a replica Domino server

1. In the server console window, type **tell sav quit**
2. Replicate the Settings and Log databases from the master Domino server to the replica Domino servers.
3. If you are prompted to overwrite an existing sav.nsf or savlog.nsf, respond **Yes**.

   This overwrites the existing databases with the new replicas.
4. Stop and restart the target Domino server.

Replicating the Definitions database

The Definitions database, savdefs.nsf, stores updated virus definitions. The database can be replicated to other Domino servers that are running Symantec AntiVirus/Filtering for Domino so that only a single LiveUpdate is required to maintain current protection on all servers.

The Domino server on which the master savdefs.nsf is created should be the computer that downloads new virus definitions updates through a scheduled LiveUpdate.

Warning: Never replicate savdefs.nsf to different operating systems. The processing engines are platform-specific.

Use of the Definitions database is only required if you plan to replicate updated virus definitions to separate physical servers. Partitioned servers on the same physical server will update definitions within ten minutes of a new LiveUpdate download. If you do not intend to replicate virus definitions, you do not need to create the Definitions database.

Warning: Never replicate savdefs.nsf to more than one partition of a multi-partition Domino server. Only one LiveUpdate per physical computer is required to update definitions on all partitions of that computer.

To prepare the Definitions database for replication

1. Select a Domino server in your organization that will be used to download updated virus definitions.
2. After you install Symantec AntiVirus/Filtering for Domino on the server, in the main window, click **LiveUpdate**.
3. On the Action bar, click **Create SAV Definitions Database**.
4. Enable and schedule the LiveUpdate.
5. Make sure that Save downloaded virus definitions in the Symantec AV/F definitions database is checked.
6. Ensure that you and LocalDomainServers are in the Access Control List of savdefs.nsf, with Manager access and Delete Documents enabled.

   The LocalDomainServers group should contain all of the servers to which you plan to replicate.

7 Create replicas of the master savdefs.nsf database on the other Domino servers that are running Symantec AntiVirus/Filtering for Domino (only one per physical computer).

   The definitions database must be in the <Domino server data directory>/sav directory on the other Domino servers and be called savdefs.nsf.

The next time that a scheduled LiveUpdate runs, any updated virus definitions are downloaded and a new savdefs.nsf document is created. The new virus definitions set is marked as active. The updated definitions are distributed to the other replicas when a manual or scheduled replication occurs. The Symantec AntiVirus/Filtering for Domino server task checks for a new virus definitions set at ten minute intervals.

After LiveUpdate runs and updates the master savdefs.nsf database, replicate the new virus definitions to other servers. Only one savdefs.nsf should exist on a single computer, regardless of the number of Notes partitions that have Symantec AntiVirus/Filtering for Domino installed.

To replicate virus definitions to other servers, do one of the following:

- Manually replicate the master savdefs.nsf to other Domino servers that are running Symantec AntiVirus/Filtering for Domino.
- Schedule the replication of the master savdefs.nsf to other Domino servers that are running Symantec AntiVirus/Filtering for Domino.

Chapter 3

Scanning for viruses

This chapter includes the following topics:

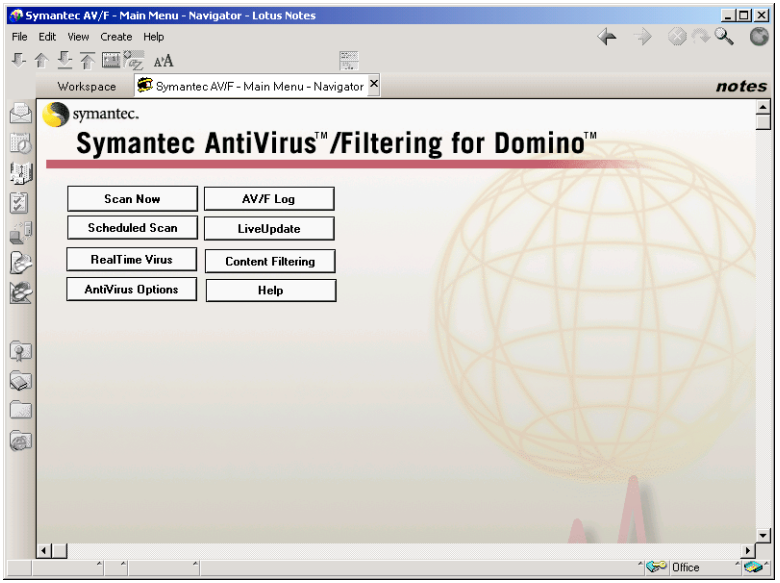
Accessing Symantec AntiVirus/Filtering for Domino

Symantec AntiVirus/Filtering for Domino runs as a Domino server task. Every time that you start the server, Symantec AntiVirus/Filtering for Domino protection begins. You access management and configuration tasks through the Lotus Notes client.

The first time you access Symantec AntiVirus/Filtering for Domino, you must also specify the server on which it is installed.

To access Symantec AntiVirus/Filtering for Domino on a Lotus Notes client

- Open the Symantec AV/F Settings database (sav.nsf) from the sav folder on the server on which it is installed.



Getting help

Symantec AntiVirus/Filtering for Domino provides an extensive system of Help topics that you can access through the Help table of contents. If you want help with a specific Symantec AntiVirus/Filtering for Domino tab, you can access context-sensitive Help for that tab when you are viewing it. If you are using the Lotus Notes client to view the Symantec AntiVirus/Filtering for Domino databases, you can also access context-sensitive Help for any options on that tab.

To get help while using Symantec AntiVirus/Filtering for Domino

- Do one of the following:
  - In the main window, click **Help** to display the Help table of contents.
  - On the Action bar of a form, click the **Help** button to access the context-sensitive Help topic.
  - On any tab that contains options, click the group label that precedes an option for a brief description of the option.

Using the Domino console window

You can view and manage some Symantec AntiVirus/Filtering for Domino operations directly from the Domino server console window.

To view and manage a Symantec AntiVirus/Filtering for Domino operation

- At the command prompt, type **TELL SAV** <command>.
  The following commands are available:

HELP	Lists Symantec AntiVirus/Filtering for Domino console commands.
INFO	Provides a summary of Symantec AntiVirus/Filtering for Domino operations.
STAT RESET	Clears processing details.
JOBS	Lists upcoming scheduled scans. The job names are entered when the scans were scheduled.
SCAN <names>	Initiates a scan of the specified databases. A number is displayed in the console window to identify each scan. If no databases are specified, only databases in the default data directory are scanned (no subdirectories are scanned). Although you can specify databases with long file names, you cannot specify file names with spaces.
STOP <n>	Stops the scan with the specified number.
QUIT	Stops the Symantec AntiVirus/Filtering for Domino server process. To reload Symantec AntiVirus/Filtering for Domino, at the console command prompt, type **LOAD NNTASK**

When you initiate scans in the console window, Symantec AntiVirus/Filtering for Domino uses Real Time settings to determine how to handle viruses. (Real Time Email Routing and Database Writes options do not need to be enabled.)

Configuring scans

Symantec AntiVirus/Filtering for Domino lets you set up scans to run immediately or on a schedule, or to monitor in real time.

You can choose from the following three types of scans, depending on the type of protection that the server requires:

- Real Time: Real Time scanning monitors database writes and email as it is routed through the server in real time. Real Time scanning is your best insurance to detect and eliminate viruses before they can spread.
  See "Scanning in real time to automatically protect against viruses" on page 31.
- Scan Now: Scan Now scans are on-demand scans that you can invoke at any time. You can include all databases in your default Data directory or select specific databases or directories to scan. The scan begins when you click Start the Scan. You can also restrict the scan to documents that have been modified before a specified date.
  See "Scanning on demand" on page 35.
- Scheduled Scans: Scheduled Scans run automatically and without administrator intervention. Use Scheduled Scans to make sure that your databases remain virus-free. You can also restrict the scan to documents that have been modified since the start time of the last Scheduled Scan.
  See "Scheduling scans" on page 40.

Note: If Symantec AntiVirus/Filtering for Domino detects a virus in an email that originated from the iNotes Web Access mail client (new in Domino R5.0.8), it logs the virus incident twice in the Symantec AntiVirus/Filtering for Domino Log database. It processes the virus detection as two separate incidents because when a user sends email using iNotes Web Access, the Lotus Domino Web server task writes the message to both the user's mail database and the Mail.box. Consequently, Symantec AntiVirus/Filtering for Domino detects a virus in both databases.

The Lotus Domino Web server task writes the iNotes Web Access email message to both databases, even when the user has set Lotus Notes Preferences not to save sent email in the user's mail database.

Scanning in real time to automatically protect against viruses

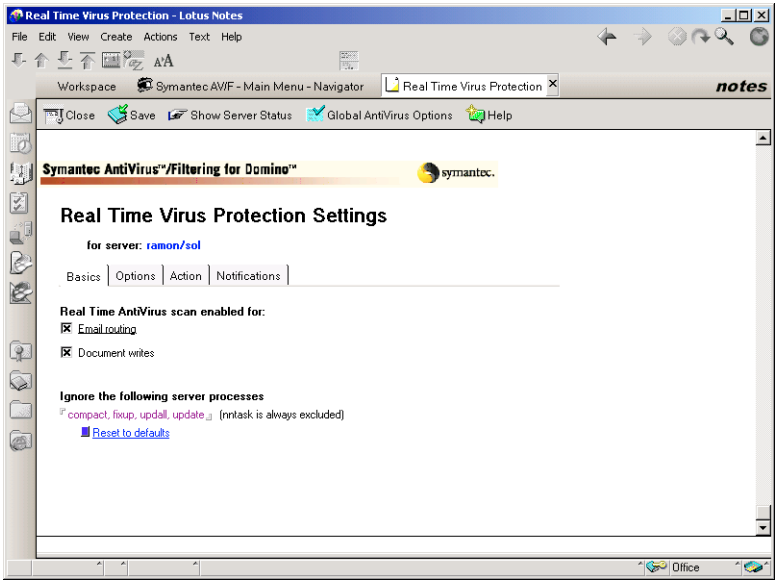
With Real Time continuous scanning, you can monitor email routing, document writes, or both. You also identify which server processes to ignore, which exclusions to apply, how to handle attachments, whether to scan for malicious HTML in the message body, and how to respond if a virus is detected.

Global AntiVirus Options that you have set apply to Real Time scanning.

See "Setting Global AntiVirus Options" on page 47.

To set up Real Time scanning

1 In the main window, click **Real Time**.



2 On the Basics tab, enable scanning.
See "Basics options for Real Time scanning" on page 32.

3 On the Options tab, specify what to scan.
See "What to Scan options for Real Time scanning" on page 33.

4 On the Action tab, specify how to respond when a virus is detected.
See "Actions options for Real Time scanning" on page 33.

5 On the Notifications tab, specify whom to alert when a virus is detected.
See "Notifications options for Real Time scanning" on page 35.

6 On the Action bar, click **Save** to save your settings.

Basics options for Real Time scanning

Table 3 describes the Basics options for Real Time scanning.

Table 3 Basics options for Real Time scanning

Enable scanning for	■ Email routing: Scans email and email attachments as they pass through the Domino server for delivery. ■ Document writes: Scans documents as they are written to server databases. By default, Symantec AntiVirus/Filtering for Domino enables both Email routing and Document writes. Uncheck both options to disable Real Time scanning.
Ignore the following server processes	Excludes the server processes that you specify from Real Time scanning. Enable this option to optimize Symantec AntiVirus/Filtering for Domino performance. By default, Symantec AntiVirus/Filtering for Domino excludes compact, fixup, updall, and update. It automatically excludes Symantec AntiVirus/Filtering for Domino processes. ■ Reset to defaults: Resets any excluded processes to their default settings.

What to Scan options for Real Time scanning

Table 4 describes the scan options for Real Time scanning.

Table 4 What to Scan options for Real Time scanning

Databases	■ Exclude specified databases and directories from scans: Excludes the databases and directories that you specify on the Options tab of Global AntiVirus Options. See "Setting Global AntiVirus Options" on page 47. Any change that you make to Global AntiVirus Options applies to all scans, not just to Real Time scanning.
Attachments	■ Scan all attachments regardless of extension: Scans all attachments. Enable this option for maximum virus protection. ■ Scan attachments with specified file extensions: Scans only attachments with the file extensions that were specified in the Specified file extensions option on the Options tab of Global AntiVirus Options. If your environment includes executable files with nonstandard extensions, add them to the list. In most cases, the default list is sufficient. Enable this option to optimize Symantec AntiVirus/Filtering for Domino performance. See "Setting Global AntiVirus Options" on page 47. Any change that you make to Global AntiVirus Options applies to all scans, not just to Real Time scanning.
Native MIME message bodies	Protects against malicious HTML commands that are embedded in MIME messages. When malicious HTML is detected, the message body can be replaced with the text that is specified on the Native MIME tab of Global AntiVirus Options. This option can slow server performance. See "Setting Global AntiVirus Options" on page 47.

Actions options for Real Time scanning

Table 5 describes the Actions options for Real Time scanning.

Table 5 Actions options for Real Time scanning

When a virus is detected	Handles a detected virus in one of the following ways: ■ Log only: Logs the detection but does nothing to the virus. ■ Delete the infected attachment: Strips the infected attachment and makes it unrecoverable. Symantec AntiVirus/Filtering for Domino adds explanatory text around the attachment icon. By default, Symantec AntiVirus/Filtering for Domino saves the deleted attachment as a Backup document in the Log/Quarantine database. When Symantec AntiVirus/Filtering for Domino detects a virus inside of a compressed file, it deletes the entire compressed file. If a compressed or encoded file is comprised of both infected and uninfected files, Symantec AntiVirus/Filtering for Domino deletes only the infected files. ■ Quarantine the document: Holds the infected document in the Log/Quarantine for administrator review. Open the AV/F Log to process infected documents. See "About the Quarantine" on page 78. ■ Repair the infected document: Eliminates the virus and repairs damage automatically. When Symantec AntiVirus/Filtering for Domino can't repair the virus, the selected If unable to repair option applies.
If unable to repair	Occasionally, Symantec AntiVirus/Filtering for Domino detects an infected document, but deems it beyond repair. When you select the Repair the infected document option, the If unable to repair option that you select applies to the scan. Otherwise, any selected If unable to repair options do not affect the scan. If unable to repair options are the following: ■ Log only: Logs the detection but does nothing to the virus. ■ Delete the infected attachment: Strips the infected attachment, making it unrecoverable. Symantec AntiVirus/Filtering for Domino adds explanatory text around the attachment icon. By default, Symantec AntiVirus/Filtering for Domino saves the deleted attachment as a Backup document in the Log/Quarantine database. When Symantec AntiVirus/Filtering for Domino detects a virus inside of a compressed or encoded file, it deletes the entire compressed file. If the file is comprised of infected, repairable, and unrepairable files, Symantec AntiVirus/Filtering for Domino repairs the repairable files and deletes everything else. ■ Quarantine the document: Holds the infected document in the Log/Quarantine for administrator review. Open the AV/F Log to process infected documents. See "About the Quarantine" on page 78.

Notifications options for Real Time scanning

Table 6 lists the Alert Messages options for sending notifications.

Table 6 Alert Messages options

Specified users (administrators and others)	Sends the alert to users who are specified in Global AntiVirus Options.
Document Author	Sends the alert to the author of the infected document or email.
Intended recipients	Sends the alert to the intended recipients of the infected email.

Status of Real Time scanning

At any time you can find out the status of Real Time scanning, including Real Time Protection settings, virus definitions, dates, last virus detected, and the number of quarantined documents.

To find out the status of Real Time scanning

1. In the main window, click **Real Time**.
2. On the Action bar, click **Show Server Status**.

Scanning on demand

Scan Now scans are on-demand scans that you can invoke at any time. With on-demand scans, you can scan all of the databases in the default data directory or selected databases and directories. Like Real Time scanning, you also specify which exclusions to apply, how to handle attachments, whether to scan for malicious HTML in the message body, whether to scan all documents or only those that have been modified since a specified date, and how to respond if a virus is detected.

Global AntiVirus Options that you have set apply to on-demand scans.

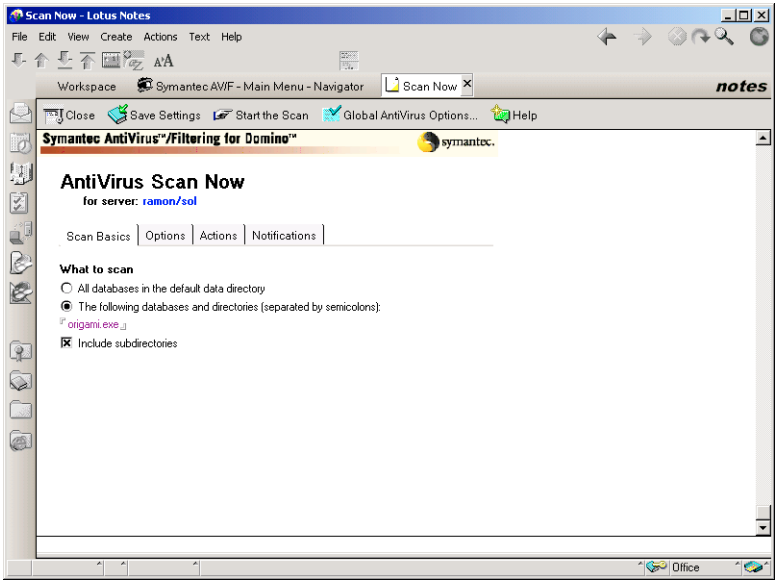
See "Setting Global AntiVirus Options" on page 47.

Run on-demand scans

After you configure a Scan Now scan, you can run it any time by clicking Start the Scan on the Action bar. You can change settings as necessary to run new on-demand scans.

To configure a Scan Now scan

1 In the main window, click **Scan Now**.



2 On the Scan Basics tab, select all or specify databases.
See "Scan Basics options for on-demand scans" on page 37.

3 On the Options tab, specify what to scan.
See "Options settings for on-demand scans" on page 38.

4 On the Actions tab, specify how to respond when a virus is detected.
See "Actions options for on-demand scans" on page 38.

5 On the Notifications tab, specify whom to alert when a virus is detected.
See "Notifications options for on-demand scans" on page 40.

6 On the Action bar, click **Save** to save your settings.

To scan on demand

1 In the main window, click **Scan Now**.

2 On the Action bar, click **Start the Scan**.

Scan Basics options for on-demand scans

Table 7 describes the Scan Basics options for on-demand scans.

Table 7 Scan Basics options for Scan Now

What to scan on the server	■ All databases in the default data directory: Scans every database in the Notes\Data directory (default location). ■ The following databases and directories: Scans only the databases that you specify. Separate multiple entries with semicolons (;). ■ Include subdirectories: Scans the descending subdirectories of the default data directory or the databases that you have specified.

Options settings for on-demand scans

Table 8 describes the Options settings for on-demand scans.

Table 8 Options settings for Scan Now

Databases	Exclude specified databases and directories from scans: Excludes databases and directories that you specify on the Options tab of Global AntiVirus Options. See "Setting Global AntiVirus Options" on page 47. Any change that you make to Global AntiVirus Options applies to all scans, not just to Scan Now scans.
Attachments	■ Scan all attachments regardless of extension: Scans all attachments. Enable this option for maximum protection. ■ Scan attachments with specified file extensions: Scans only attachments with the file extensions that were specified in the Specified file extensions option on the Options tab of Global AntiVirus Options. If your environment includes executable files with nonstandard extensions, add them to the list. In most cases, the default list is sufficient. Enable this option to optimize Symantec AntiVirus/Filtering for Domino performance. See "Setting Global AntiVirus Options" on page 47. Any change that you make to Global AntiVirus Options applies to all scans, not just to Scan Now scans.
Native MIME message bodies	Protects against malicious HTML commands that are embedded in MIME messages. When malicious HTML is detected, the message body can be replaced with the text that is specified on the Native MIME tab of Global AntiVirus Options. This option can slow server performance. See "Setting Global AntiVirus Options" on page 47.
Incremental Scan	Limits the scan to documents that are modified after the date that you specify. Symantec AntiVirus/Filtering for Domino uses the user's current date format regardless of what you type. For example, if you typed 5-3-02 12 AM, and the user's date format is MM-DD-YY HH:MM AM/PM, Symantec AntiVirus/Filtering for Domino reflects the date 05-03-02 12:00 AM.

Actions options for on-demand scans

Table 9 describes the Actions options for on-demand scans.

Table 9 Actions options for Scan Now

When a virus is detected	Handles a detected virus in one of the following ways: ■ Log only: Logs the detection but does nothing to the virus. ■ Delete the infected attachment: Strips the infected attachment and makes it unrecoverable. Symantec AntiVirus/Filtering for Domino adds explanatory text around the attachment icon. By default, Symantec AntiVirus/Filtering for Domino saves the deleted attachment as a Backup document in the Log/Quarantine database. When Symantec AntiVirus/Filtering for Domino detects a virus inside of a compressed file, it deletes the entire compressed file. If a compressed or encoded file is comprised of both infected and uninfected files, Symantec AntiVirus/Filtering for Domino deletes only the infected files. Explanatory text does not apply to any files deleted in a container file. ■ Quarantine the document: Holds the infected document in the Log/Quarantine for administrator review. Open the AV/F Log to process infected documents. See "About the Quarantine" on page 78. ■ Repair the infected document: Eliminates the virus and repairs damage automatically. When Symantec AntiVirus/Filtering for Domino can't repair the virus, the selected If unable to repair option applies.
If unable to repair	Occasionally, Symantec AntiVirus/Filtering for Domino detects an infected document, but deems it beyond repair. When you select the Repair the infected document option, the If unable to repair option that you select applies to the scan. Otherwise, any selected If unable to repair options do not affect the scan. If unable to repair options are the following: ■ Log only: Logs the detection but does nothing to the virus. ■ Delete the infected attachment: Strips the infected attachment and makes it unrecoverable. Symantec AntiVirus/Filtering for Domino adds explanatory text around the attachment icon. By default, Symantec AntiVirus/Filtering for Domino saves the deleted attachment as a Backup document in the Log/Quarantine database. When Symantec AntiVirus/Filtering for Domino detects a virus inside of a compressed or encoded file, it deletes the entire compressed file. If the file is comprised of infected, repairable, and unrepairable files, Symantec AntiVirus/Filtering for Domino repairs the repairable files and deletes everything else. ■ Quarantine the document: Holds the infected document in the Log/Quarantine for administrator review. Open the AV/F Log to process infected documents. See "About the Quarantine" on page 78.

Notifications options for on-demand scans

Table 10 lists the Alert Messages options for sending notifications.

Table 10 Alert Messages options

Specified users (administrators and others)	Sends the alert to users that are specified in Global AntiVirus Options.
Document Author	Sends the alert to the author of the infected document or email.

Scheduling scans

You can schedule scans to repeat at the same time on specified days or at a specified interval on specified days.

To configure a Scheduled Scan, you specify the days and times to run the scan, including whether to run after a virus definitions update with LiveUpdate. You also specify which databases to scan, which exclusions to apply, how to handle attachments, whether to scan all documents or only those that have been modified since the last scheduled scan, and how to respond if a virus is detected. You can enable or disable individual Scheduled Scans.

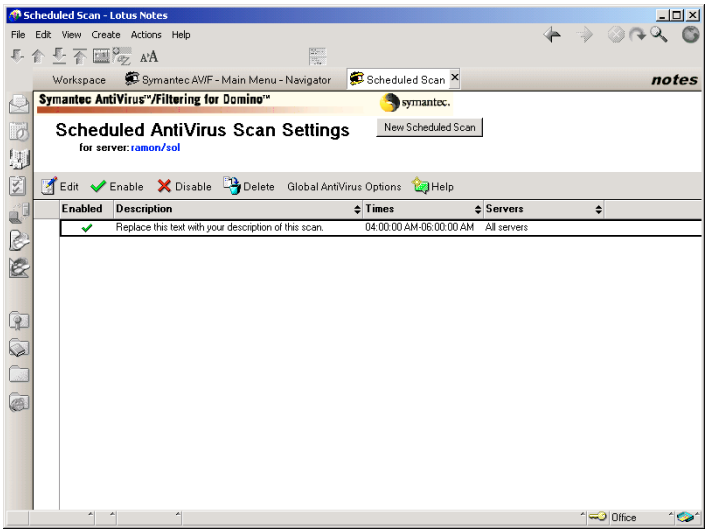
Global AntiVirus Options that you have set apply to Scheduled Scans.

See "Setting Global AntiVirus Options" on page 47.

Note: For domains with multiple servers, Symantec AntiVirus/Filtering for Domino provides an option to schedule the same scan to run on one or more servers. You can schedule the scan from any server in the domain. For server-specific changes to scheduled scans, the sav.nsf database must be replicated to the appropriate servers.

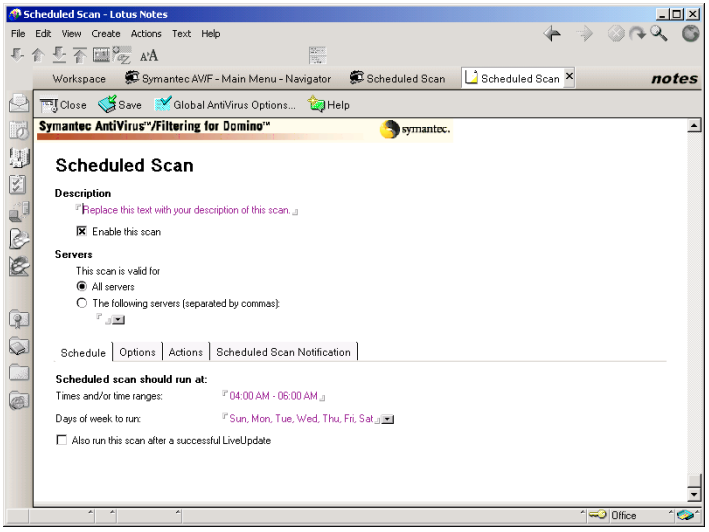
To schedule or modify a scan

1 In the main window, click **Scheduled Scan** to display the current scanning schedule.



2 Do one of the following:

- To set up a new Scheduled Scan, on the Action bar, click **New Scheduled Scan.**
- To modify an existing scan, double-click the scan.



3 Under Description, type a description to identify the Scheduled Scan in the listing of Scheduled Scans.

4 Check **Enable this scan**.

5 Under Servers, select one of the following:

- All servers: Runs the scan on every server.
- The following servers: Runs the scan on only the servers that you specify. Separate multiple entries with commas. The Browse button beside the field opens a list from which you can select servers.

6 On the Schedule tab, specify the scan times.

In a high-traffic network, schedule system-wide scans to run at off-peak times. For critical databases, schedule frequent scans. Schedule scans to run before database backups.

See "Schedule options for Scheduled Scans" on page 43.

7 On the Options tab, specify what to scan.

See "Options for Scheduled Scans" on page 44.

8 On the Actions tab, specify how to respond when a virus is detected.

See "Actions options for Scheduled Scans" on page 45.

9 On the Scheduled Scan Notification tab, specify whom to alert when a virus is detected.

See "Scheduled Scan Notification options" on page 46.

10 On the Action bar, click **Save** to save your settings.

Schedule options for Scheduled Scans

Table 11 lists the Schedule options for Scheduled Scans.

Table 11 Schedule options for Scheduled Scans

Days of the week to run	Scans on the days of the week that you check.
Times and/or time ranges	Scans during the times or time ranges that you enter. You can enter a single time for the scan to start or time ranges for the scan to start and stop. When you enter a single time, for example, 9:00 AM, the scan always continues to completion, regardless of the time that is required to do so. However, when you enter a time range, for example, 04:00-06:00 AM, the scan starts at 04:00 AM, and completes at 06:00 AM, even if it has not finished scanning all of the databases that it was configured to scan. When a scan has remaining databases to examine at its stop time, it will continue where it left off at the next schedule time. This capability ensures coverage for sites with many large databases, but not enough available time intervals to complete large scans at any one time. Separate time ranges with semicolons (for example, 4-6; 8-10). By default, Symantec AntiVirus/Filtering for Domino is configured to run a Scheduled Scan daily between 04:00 AM and 06:00 AM. (You must enable this scan before it can run.)
Also run this scan after a successful LiveUpdate	Scans immediately after virus definitions files are updated. Enable this option to protect against newly discovered viruses. For this option to work, you must have enabled LiveUpdate. See "Maintaining current protection" on page 89.

Options for Scheduled Scans

Table 12 lists the Options for Scheduled Scans.

Table 12 Options for Scheduled Scans

What to scan during the Scheduled Scan	■ All databases in the default directory: Scans every database in the Notes\Data directory (default location) on the server. ■ The following databases and directories: Scans only the databases that you specify. Separate multiple entries with semicolons (;). ■ Include subdirectories: Scans the descending subdirectories of the default data directory or the databases that you have specified.
Databases	Excludes databases and directories that are specified in Global AntiVirus Options. If your environment includes executable files with nonstandard extensions, add them to the list. In most cases, the default list is sufficient. Enable this option to optimize Symantec AntiVirus/Filtering for Domino performance. See "Setting Global AntiVirus Options" on page 47. Any change that you make to Global AntiVirus Options applies to all scans, not just to Scheduled Scans.
Attachments	■ Scan all attachments regardless of extension: Scans all attachments. Enable this option for maximum protection. ■ Scan attachments with specified file extensions: Scans only those attachments with file extensions that are specified in the Specified file extensions option on the Options tab of Global AntiVirus Options. If your environment includes executable files with nonstandard extensions, add them to the list. In most cases, the default list is sufficient. Enable this option to optimize Symantec AntiVirus/Filtering for Domino performance. See "Setting Global AntiVirus Options" on page 47. Any change that you make to Global AntiVirus Options applies to all scans, not just to Scheduled Scans.

Native MIME message bodies	Protects against malicious HTML commands that are embedded in MIME messages. When malicious HTML is detected, the message body can be replaced with the text that is specified on the Native MIME tab of Global AntiVirus Options. This option can slow server performance. See "Setting Global AntiVirus Options" on page 47. Any change that you make to Global AntiVirus Options applies to all scans, not just to Scheduled Scans.
Incremental Scan	Limits the scan to documents that were modified after the last (indicated) Scheduled Scan. Enabling this option prevents rescanning of file documents. ■ Reset incremental scan date: Resets the date to scan all attachments on the next Scheduled Scan date.

Actions options for Scheduled Scans

Table 13 lists the Actions options for Scheduled Scans.

Table 13 Actions options for Scheduled Scans

When a virus is detected	Handles a detected virus in one of the following ways: ■ Notify only: Logs the detection but does nothing to the virus. ■ Delete the infected attachment: Strips the infected attachment and makes it unrecoverable. Symantec AntiVirus/Filtering for Domino adds explanatory text around the attachment icon. By default, Symantec AntiVirus/Filtering for Domino saves the deleted attachment as a Backup document in the Log/Quarantine database. When Symantec AntiVirus/Filtering for Domino detects a virus inside of a compressed file, it deletes the entire compressed file. If a compressed or encoded file is comprised of both infected and uninfected files, Symantec AntiVirus/Filtering for Domino deletes only the infected files. ■ Quarantine the document: Holds the infected document in the Log/Quarantine for administrator review. Open the AV/F Log to process infected documents. See "About the Quarantine" on page 78. ■ Repair the infected document: Eliminates the virus and repairs damage automatically. When Symantec AntiVirus/Filtering for Domino can't repair the virus, the selected If unable to repair option applies.

If unable to repair	Occasionally, Symantec AntiVirus/Filtering for Domino detects an infected document, but deems it beyond repair or does not remove the virus because it resides within a compressed file (for example, a .zip file). In such cases, you must first decompress the compressed file before Symantec AntiVirus/Filtering for Domino can repair the damage. When you select the Repair the infected document option, the If unable to repair option that you select applies to the scan. Otherwise, any selected If unable to repair options do not affect the scan. If unable to repair options are the following: ■ Notify only: Logs the detection but does nothing to the virus. ■ Delete the infected attachment: Strips the infected attachment and makes it unrecoverable. Symantec AntiVirus/Filtering for Domino adds explanatory text around the attachment icon. By default, Symantec AntiVirus/Filtering for Domino saves the deleted attachment as a Backup document in the Log/Quarantine database. When Symantec AntiVirus/Filtering for Domino detects a virus inside of a compressed or encoded file, it deletes the container and the files inside it. If the files are comprised of infected, repairable, and unrepairable files, Symantec AntiVirus/Filtering for Domino repairs the repairable files and deletes everything else. ■ Quarantine the document: Holds the infected document in the Log/Quarantine for administrator review. Open the AV/F Log to process infected documents. See "About the Quarantine" on page 78.

Scheduled Scan Notification options

Table 14 lists the Alert Messages options for sending notifications.

Table 14 Alert Messages options

Specified users (administrators and others)	Sends the alert to users who are specified in Global AntiVirus Options.
Document Author	Sends the alert to the author of the infected document or email.

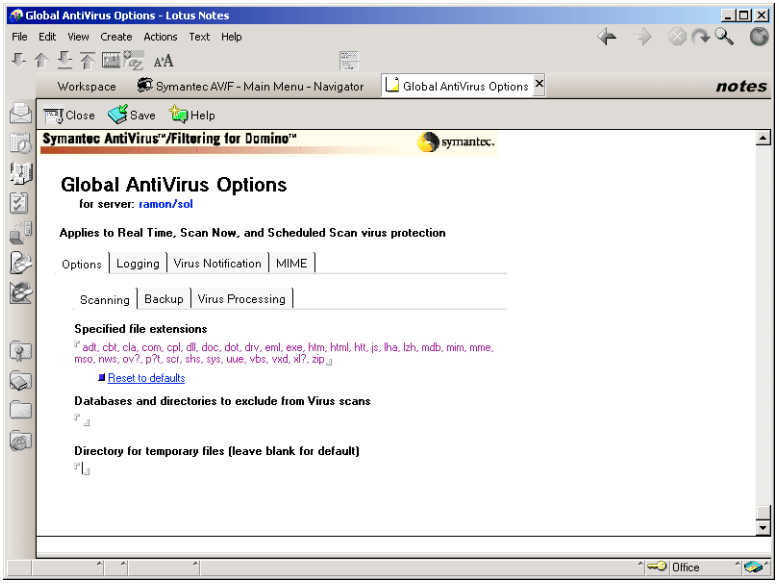
Setting Global AntiVirus Options

Global AntiVirus Options let you specify various settings that apply to all scans (such as the databases and file extensions to exclude from scans). When you specify settings in Global AntiVirus Options, the settings apply to Real Time scanning, all Scan Now scans, and all Scheduled Scans. Changes made, for example, while you are setting up Global AntiVirus Options for an on-demand (Scan Now) scan, also apply to Real Time scanning and Scheduled Scans. Once they are set, you probably won't need to change Global AntiVirus Options.

To set Global AntiVirus Options

1 Do one of the following:

- In the main window, click **AntiVirus Options.**
- In a Scan Now, Scheduled Scan, or Real Time scanning settings document, on the Action bar, click **Global AntiVirus Options**.



2 On the Options tab, set Scanning, Backup, and Virus Processing options.
See "Global Options settings: Scanning options" on page 49.
See "Global Options settings: Backup options" on page 50.
See "Global Options settings: Virus Processing options" on page 50.

3 On the Logging tab, specify what to log.
See "Global Logging settings" on page 51.

4 On the Virus Notification tab, specify whom to notify when a virus is detected.
See "Global Virus Notification settings" on page 51.

5 On the MIME tab, specify replacement text as necessary.
See "Global Native MIME settings" on page 53.

6 On the Action bar, click **Save** to save your settings.

Global Options settings

The Global Options settings tab includes three subtabs:

- Scanning
- Backup
- Virus Processing

Global Options settings: Scanning options

Table 15 lists the inclusions and exclusions settings for Global AntiVirus Options.

Table 15 Options settings for Global AntiVirus Options

Specified file extensions	When Scan Attachments With Specified Extensions is selected on the Real Time, Scan Now, or Scheduled Scans forms, only attachments with listed file extensions are scanned. This setting reduces resource demand and speeds processing during the scan. The default list includes file types that are commonly at risk of infection. If your environment includes executable files with nonstandard extensions, add them to the list. In most cases, however, the default list is sufficient. When compressed files (for example, .zip files) are scanned and this option has been enabled, Symantec AntiVirus/Filtering for Domino scans the container and the files inside of it only if you have specified the extension of the compressed file in the list (for example, .zip). ■ Reset to defaults: Resets specified file extensions to their default settings.
Databases and directories to exclude from scans	When Exclude specified databases and directories from scans is checked on the Real Time, Scan Now, or Scheduled Scans forms, the listed databases and directories are skipped. For example, you may have documentation or reference databases that are not at risk of virus infection because they cannot be modified by users. Separate multiple entries with semicolons (;). Do not use wildcards.
Directory for temporary files (Leave blank for default)	Specifies the directory to use for temporary files. Symantec AntiVirus/Filtering for Domino uses the default Windows TEMP directory for processing during scans. You should have at least 100 MB of free space on the drive that contains this directory. If necessary, you can specify a directory on another drive that has more space. If you enter a directory that is invalid, Symantec AntiVirus/Filtering for Domino defaults to the Windows TEMP directory. If you use a non-Symantec antivirus product, disable scanning of this directory to prevent interference with Symantec AntiVirus/Filtering for Domino operation.

Global Options settings: Backup options

Table 16 lists the Backup options for Global AntiVirus Options.

Table 16 Backup Global AntiVirus Options

Back up documents before repairing attachments	■ Yes: As a data safety precaution, stores a backup copy of an infected document before repairing it. In the AV/F Log, click Backup documents to view the list and delete or restore backups. ■ No: Repairs the infected document without making a backup copy.
Back up documents before deleting attachments	■ Yes: As a data safety precaution, stores a backup copy of an infected document before deleting its infected attachment. In the AV/F Log, click Backup documents to view the list and delete or restore backups. ■ No: Deletes the attachments without making a backup copy of the document.

Global Options settings: Virus Processing options

Table 17 lists the AntiVirus Engine options for Global AntiVirus Options.

Table 17 AntiVirus Engine Global AntiVirus Options

Bloodhound heuristic virus detection technology	Sets the level of resource demand from Bloodhound. Bloodhound is an advanced heuristic technology that detects a high percentage of new or unknown viruses that have not yet been analyzed by antivirus researchers. Because Bloodhound requires only a small processing overhead, you can set a resource demand level. In most cases, the Med (medium) setting is appropriate.
Repair signed documents (will break signatures on repaired documents)	Repairs ID-signed documents, but not X.509 Certificate-signed documents. To eliminate viruses from ID-signed documents, Symantec AntiVirus/Filtering for Domino must break the signature. When enabled, Symantec AntiVirus/Filtering for Domino breaks the signature and repairs the document. When this option is disabled and Symantec AntiVirus/Filtering for Domino detects a virus in an ID-signed document, it treats the document as unrepairable. If this option is disabled and you have selected the Repair the infected attachment on any of the scan forms (Real Time, Scan Now, or Scheduled Scans), Symantec AntiVirus/Filtering for Domino handles the ID-signed document according to the If unable to Repair setting.

Global Logging settings

Table 18 lists the Logging options for Global Options.

Table 18 Logging Group Options

Log the following messages	Determines which messages and virus events are logged.

Global Virus Notification settings

Table 19 lists the Global Virus Notification options.

Table 19 Virus Notification options

Administrators	Specifies the email alert to send to administrators to advise them of infected workstations. The options are as follows: ■ Send email alerts to the following users: Sends alerts to specified administrators. ■ Custom text to specified administrators: Specifies the subject line and body content of the email message that is sent for the alert that was generated. Use tokens to customize the subject or body of the email alert as necessary. See "Tokens for customizing email alerts" on page 52. ■ Report action taken by Symantec AntiVirus/Filtering for Domino: Includes the action that was taken by Symantec AntiVirus/Filtering for Domino in the email to the administrator. ■ Include violation information from the log: Includes information about the violation from the Log.

Document Author	Specifies the email alert to send to the author of the infected document. If your policy is to quarantine infected documents, let authors know whom to contact to release the document. If your policy is to delete infected attachments, advise authors to scan the source before sending the attachment again. The options are as follows: ■ Send email alerts to document author: Sends alerts to the document author. ■ Custom text to document author: Specifies the subject line and body content of the email message that is sent for the alert that was generated. Use tokens to customize the subject or body of the email alert as necessary. See "Tokens for customizing email alerts" on page 52. ■ Report action taken by Symantec AntiVirus/Filtering for Domino: Includes the action that was taken by Symantec AntiVirus/Filtering for Domino in the email to the document author. ■ Include violation information from the log: Includes information about the violation from the Log in the email to the document author.
Document Recipients	Specifies the email alert to send to the intended recipients of the infected document. If your policy is to quarantine infected documents, let users know whom to contact to release the document. If your policy is to delete infected attachments, advise them to contact the document author to resend an uninfected version. The options are as follows: ■ Send email alerts to intended recipients: Sends the alert to the intended recipients of the document. ■ Custom text to intended recipients: Specifies the subject line and body content of the email message that is sent for the alert that was generated. Use tokens to customize the subject or body of the email alert as necessary. See "Tokens for customizing email alerts" on page 52. ■ Report action taken by Symantec AntiVirus/Filtering for Domino: Includes the action that was taken by Symantec AntiVirus/Filtering for Domino in the email to the recipient. ■ Include violation information from the log: Includes information about the violation from the Log.

Tokens for customizing email alerts

To create email alerts more efficiently, you can substitute tokens to represent custom text. For example, %Author% displays the author's name.

Table 20 lists tokens to help you customize email alerts.

Table 20 Tokens available for customizing email alerts

Token	Description
%DBName%	Document's database name.
%DBTitle%	Document's database title.
%DocumentUniqueID%	Unique ID of the document (UNID).
%NoteID%	NOTEID of the document.
%Author%	Most recent author of the document.
%Created%	Creation time and date of the document.
%Modified%	Time and date of the last modification to the document.
%Accessed%	Time and date that the document was last accessed.
%InfectedAttachment%	Name of the first infected attachment.
%Virus%	Name of the first virus found.
%<fieldname>%	Value of the <fieldname> in the document. When a document does not contain a specified field, leave the token blank.

Global Native MIME settings

Table 21 lists the Native MIME options for Global AntiVirus Options.

Table 21 Native MIME options

Replace deleted MIME message bodies with the following text	When a scan (Real Time, Scan Now, or Scheduled Scan) has been configured to delete the infected attachment when a virus is detected, Symantec AntiVirus/Filtering for Domino deletes the entire message body of the infected, native MIME message and replaces it with the default text or the text that you specify. Infected native MIME messages cannot be repaired.

Optimizing performance

You can manage resource demand during scans by selecting the following options when you configure scans:

- Scan only specified file extensions when configuring scans: The default list of extensions includes the file types commonly at risk of infection. Select the Scan All Attachments option if you have virus problems that are not under control.
- Exclude from scans those databases that are unlikely to become infected: You may have documentation or reference databases that are not at risk of virus infection because they cannot be modified by users.

To view or modify the list of file extensions or excluded databases for scans

- In the main window, click **AntiVirus Options** to access Global AntiVirus Options.

Chapter 4

Filtering content

This chapter includes the following topics:

About content filtering

Content filtering is typically used to monitor the mail system and block messages that contain specific types of content. For example, in most organizations, sending messages with explicit sexual or violent content is not appropriate, and violates corporate conduct guidelines. In other cases, an organization may want to prevent the spread of confidential information outside of the organization, or block messages that could have legal consequences.

The rules also provide a front-end defense against spam. Because it is proactive, content filtering can identify and block the spread of new, unknown viruses before updated virus definitions files are available. These rules give administrators more control to block objectionable email and other documents that are created in Lotus Notes databases.

How content filtering works

Email or database writes that match an expression in a Content Rule may violate the rule, depending on whether the rule contains AND expressions or OR expressions. If the rule contains AND expressions, then all expressions must evaluate to true for Symantec AntiVirus/Filtering for Domino to trigger a content violation for the entire rule. However, if the rule contains OR expressions, only one expression must evaluate to true for Symantec AntiVirus/Filtering for Domino to trigger a content violation for the rule.

You can change, delete, enable, or disable any rules that you create.

See "The elements of a Content Filtering Rule" on page 57.

Symantec AntiVirus/Filtering for Domino handles email with content violations according to the action that you configure for the rule. You can choose one of the following actions (one action per rule):

- Log only: Logs the content violation in the Symantec AntiVirus/Filtering for Domino Log database, but does nothing else.
- Delete the offending attachments: Deletes only the attachment or attachments that have violated (or matched) the rule. The condition or conditions of the rule itself must specify the attachment name, size, extension, and so forth, or this action won't work.
- Delete all attachments: Deletes every attachment that belongs to the email, regardless of which attachment or attachments contain the content violation.
- Quarantine the document: Moves the email to the Log/Quarantine database and lists it as a Quarantined item.

- Copy the document: Copies the email to the Log/Quarantine database and lists it as a Backed Up Document. The email does not appear in the Quarantined item list.
- Delete the document: Deletes the email, including any attachments.

Administrators can also notify authors, recipients, or others of content filtering violations using messages with customizable text. To set up notification, administrators must configure an alert.

When enabled, Symantec AntiVirus/Filtering for Domino performs content filtering during any of the scan types for which Symantec AntiVirus/Filtering for Domino provides alert notification (Scan Now scans, Scheduled Scans, and Real Time scanning).

The elements of a Content Filtering Rule

A Content Filtering Rule consists of one or more expressions that you define. For example, the following Content Filtering Rule contains three expressions that filter for Subject line content or .exe attachments unless the body contains particular text:

If Subject Contains [Ignore case] [Winner] OR Attachment ext. =[exe] UNLESS Body Contains [Ignore case] [Email test from the lab]

An expression consists of one or more expression phrases. Expression phrases can be IF, OR, AND, or UNLESS phrases. The rule above consists of an IF, an OR, and an UNLESS phrase.

Symantec AntiVirus/Filtering for Domino evaluates a rule logically as either an OR or AND rule, but not in combination. You can have a rule that contains an IF phrase, any number of AND phrases, and any number of UNLESS phrases, but it cannot contain an OR phrase if it already has an AND phrase. Similarly, if you start with an OR phrase, you can add more OR phrases or UNLESS phrases, but you cannot include an AND phrase.

An expression phrase consists of the following elements:

- Attribute: The part or characteristic of the email or document that you want to scrutinize for violations. Attributes include Sender, Subject, Body, Size (of the entire email or document, in bytes), Encryption flag (true or false), Internet domain, Domino domain, Attachment name, Attachment name extension, or Attachment size (in bytes).
- Operator: The comparison that you want to make between the attribute and the value that, when matched to the Attribute, constitutes a content violation. Operators include Contains, Does not contain, = (equals), <> (does not equal), > (greater than), < (less than), True, and False. The availability of certain Operators is limited by which Attribute is selected.
- Value: The numeric value or alphanumeric text string that you enter as the criteria to match. The Attributes of Size and Attachment size take numeric values. The rest (except Encryption Flag) take alphanumeric text strings. The Encryption flag Attribute takes the Boolean values of True or False.

The Attribute that you select determines which operators you can use. Some Attributes have more operators than others. For example, if you select Sender/Author as the Attribute, then the available operators are Contains, Does not contain, =, and <>. However, if you choose Encryption Flag as the attribute, then only the = operator is available.

Most Attributes (Attachment name, Attachment ext., Body, Domino Domain, Domino Server, Internet Domain, Sender/Author, and Subject) take alphanumeric text strings as their values. This means that even if you typed a number in the Value field, Symantec AntiVirus/Filtering for Domino would consider it text, not a number. Because they allow for regular expressions, text strings give you flexibility to extend your text searches to find more than just a direct match. Regular expressions include metacharacters, or wildcards, to broaden the search capabilities of a given rule.

About regular expressions

A regular expression is a set of symbols and syntactic elements that is used to match patterns of text. Symantec AntiVirus/Filtering for Domino performs matching on a line-by-line basis. It does not evaluate the line feed (newline) character at the end of each input expression phrase.

You can build regular expressions using a combination of normal alphanumeric characters and metacharacters also called wildcards. Wildcards let you perform pattern matching in text. For example, spam often contains a trailing number at the end of the subject line, as in the following example:

Here's a hot stock pick!43234

To write a rule to match email subject lines that have trailing numbers, compare the subject against the following regular expression:

.+[0-9]+

This regular expression contains the normal alphanumeric characters 0-9 and the metacharacters (wildcards) ^, ., +, and []. By using the Subject Attribute, the = operator, and the regular expression above as the Value, you can build a Content Filtering Rule to catch any email messages with subject lines that end with a trailing number.

For more information, see "About metacharacters" on page 59.

In another example, you may want to filter any email messages with certain attachment extension names. To catch messages whose attachment extensions are .exe, .com, or .zip, you could write three different expressions phrases, each focusing on one of the extensions. A more practical and faster way to do it, however, is to use the pipe metacharacter (|), which creates an OR expression, for example:

Attachment ext. = com|exe|zip

This example matches any first-level extension names that equal .com, .exe, or .zip.

Note: For content filtering only, first-level attachments refer to the outer-most file attachment. The content filtering engine does not evaluate any file extension names inside the outer attachment, for example, the compressed files in a .zip file.

About metacharacters

Table 22 lists the metacharacters that you can use in regular expressions to build Content Filtering Rules. Some characters are not considered special unless you use them in combination with other characters.

Note: You can use metacharacters in regular expressions to search for single-byte and multi-byte character patterns. However, if you create a regular expression in which you specify a character range, the character that you use to specify the range must be a single-byte character.

For example, in the regular expression x{4}, x must be a single-byte character. Similarly, in x{10, 15}, x must be a single-byte character. In the regular expression [string], string must contain only single-byte characters.

Table 22 Metacharacters for use in regular expressions

Metacharacter	Description
.	Period: Matches any single character of the input sequence.
^	Caret: Represents the beginning of the input. For example, ^A is a regular expression that matches the letter A at the beginning of the field. The ^ character is only special at the beginning of a regular expression or after the (or | characters. **Note:** When performing an 'equals' comparison, the ^ character is added automatically to the beginning of the regular expression or pattern and the $ character is added automatically to the end. Only use the ^ and $ characters with 'contains' or expressions other than 'equals'.
$	Dollar sign: Represents the end of the input. For example, A$ is a regular expression that matches the letter A at the end of the field. The $ character is only special at the end of a regular expression or before the) or | characters. **Note:** When performing an 'equals' comparison, the ^ character is added automatically to the beginning of the regular expression or pattern and the $ character is added automatically to the end. Only use the ^ and $ characters with 'contains' or expressions other than 'equals'.
*	Asterisk: Matches zero or more instances of the string to the immediate left of the asterisk. For example, A* matches A, AA, AAA, and so on. It also matches the null string (zero occurrences of A).
?	Question mark: Matches zero or one instance of the string to the immediate left of the asterisk.
+	Plus sign: Matches one or more instances of the string to the immediate left of the plus sign.
\	Escape: Turns on or off the special meaning of metacharacters. For example, \. only matches a dot character. \$ matches a literal dollar sign character. Note that \\ matches a literal \ character.

Metacharacter	Description
|	Pipe: Matches either expression on either side of the pipe. For example, exe|com|zip matches exe, com, or zip.
[string]	Brackets: Inside the brackets, matches a single character or collating element, as in a list. The string inside the brackets is evaluated literally, as if an escape character (\) were placed before each character in the string. ■ If the initial character in the brackets is a caret (^), then the expression matches any character or collating element except those inside the bracket expression. ■ Specify character ranges with a dash (-) between two characters or collating sequences to indicate the range of all characters or collating sequences between the explicit ones on either side of the dash. The range does not refer to the native character set. For example, in the POSIX locale, [a-z] means all lowercase letters even when they don't agree with the binary machine ordering. However, because many other locales do not collate in this manner, do not use ranges in strictly conforming POSIX.2 applications. A collating sequence may explicitly be an endpoint of a range. For example, [[.ch.]-[.11.]] is valid; however, equivalence or character classes may not be valid. For example, [[=a=]-z] is illegal. ■ If the first character after any caret (^) is a dash (-) or a closing bracket (]), then that character matches only a literal dash or closing bracket.
char{n}	A single character (char) followed by a number (n) in braces: Matches the number of repetitions of the character. For example, X{3} matches XXX.
char{min,}	A single character (char) followed by a number (min) and a comma in braces: Matches the minimum number of repetitions of the character. For example, X{3,} matches at least three repetitions of X.

Metacharacter	Description
char{min,max}	A single character (char) followed by a pair of numbers in braces: Matches the minimum number of repetitions of the character but no more than the maximum number of repetitions. For example, X{3,7} matches from three to seven repetitions of X.
(string)	Parentheses: Groups parts of regular expressions, which gives the string inside the parentheses precedence over the rest.

The order of metacharacters, from highest to lowest precedence, is shown in Table 23.

Table 23 Precedence of metacharacters

Metacharacter	Meaning
()	Precedence override
|	OR
[]	List
\	Escape
^	Start with

Examples of regular expressions using metacharacters

You can link several regular expressions to form a larger one. Table 24 shows examples of regular expressions that demonstrate how pattern matching is accomplished with the use of metacharacters of regular alphanumeric characters.

Table 24 Examples of regular expressions

Regular expression	Meaning
abc	Matches any line of text that contains the three letters abc in order.
a.c	Matches any string that begins with the letter a, followed by any character, followed by the letter c.
c$	Matches any line that ends with the letter c.
a(b*|c*)d	Matches any string that begins with the letter a, followed by either zero or more instances of the letter b, or zero or more instances of the letter c, followed by the letter d.
.* [a-z]+ .*	Matches any line that contains a word that consists of lowercase alphabetic characters, delimited by at least one space on each side. In this example, there is a space before the [character and a space after the + character.
.*monti.*monti.*	Matches lines that contain at least two occurrences of the string monti.
[[:space:][:alnum:]]	Matches any character that is either a whitespace character or alphanumeric.

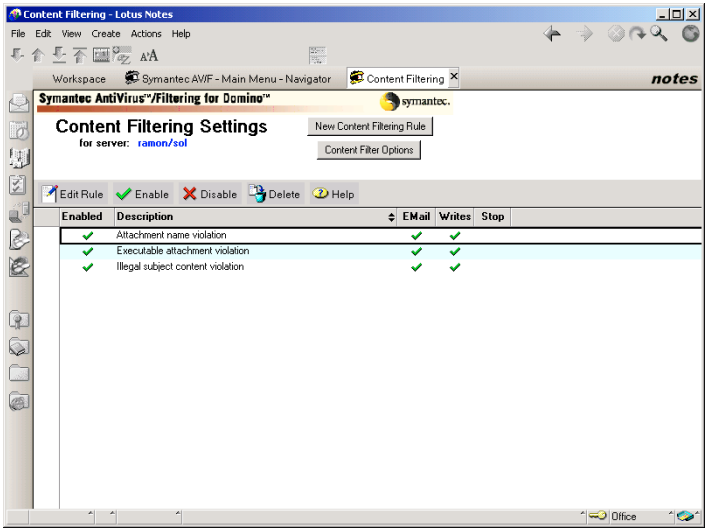
Defining and modifying Content Filtering Rules

To create a rule, you specify the basics and then set up as many conditional expressions as required to categorize the objectionable content that you are trying to block. You can then specify how to handle the document (or attachment) that contains objectionable content.

When you are ready to process a Rule, make sure that it is enabled individually on the Basics tab. Then, on the Rules tab, which lists the Rules, enable Rules processing.

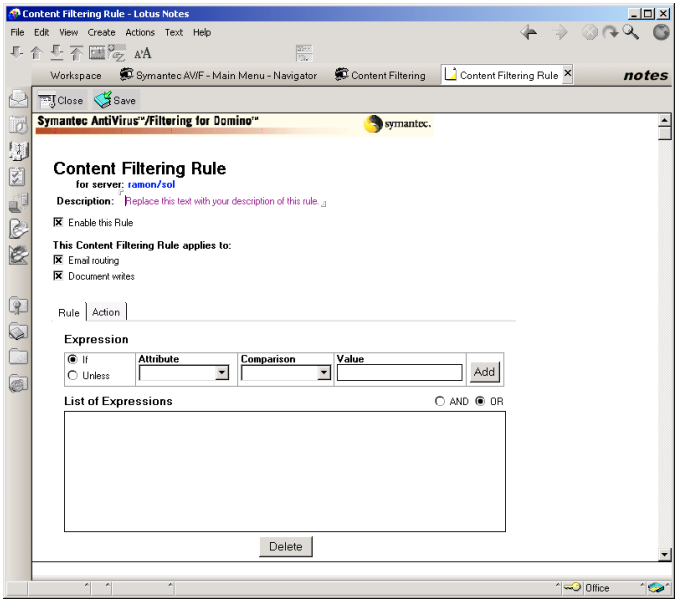
To define or modify a Content Filtering Rule

1 In the main window, click **Content Filtering**.



2 In the Content Filtering Settings window, do one of the following:

- Click **New Content Filtering Rule**.
- Double-click an existing Content Filtering Rule.



3 In the Content Filtering Rule window, set the basic options.
See "Basic options for content filtering" on page 65.

4 On the Rule tab, define the rule by building it from one or more expressions.
See "Rules options for content filtering" on page 65.
For attributes that take text strings, you can build regular expressions using metacharacters to extend your text matches.
See "About regular expressions" on page 58.

5 On the Action tab, set the action options.
See "Action options for content filtering" on page 67.

6 On the Action bar, click **Save** to save your settings.

Basic options for content filtering

Table 25 lists the basic options for content filtering.

Table 25 Content filtering basic options

Description	Provides a place to specify a meaningful name for the Content Filtering Rule so that you can identify it in the list of rules and in the Log.
Enable this Rule	Enables the current Content Filtering Rule after it is saved.
This content Filtering rule applies to	■ Email Routing: Applies the Content Filtering Rule to all email that passes through the server. ■ Document writes: Applies the Content Filtering Rule to databases on the server.

Rules options for content filtering

Table 26 lists the Rules options for content filtering.

Table 26 Content Filtering Rules options

Expression	Lets you create one or more conditional expressions that define the Content Filtering Rule: ■ If: Sets up the expression to be a condition of the Content Filtering Rule. You must create at least one IF expression. ■ Unless: Sets up the expression to be an exception to all conditional (IF) expressions above it. ■ Attribute: Selects the basis for the rule. For example, if you select Body as the attribute, the Content Filtering Rule will involve only the body of an email message. Specifying Attachment size as the attribute limits the rule to violations in the file sizes of email attachments, and so on. ■ Comparison: Selects the relationship between the attribute (subject) of the rule and the value. Available Comparison options change, depending on the attribute selected. For example, if you select Size as the attribute, your available Comparison options are > (greater than), < (less than), = (equal to), and <> (not equal to). Other attributes may yield different sets of options. When you select the Body attribute along with the Comparison options, you also see an option to ignore the case, which allows you to specify a value in any combination of uppercase or lowercase letters. ■ Value: Specifies the word, phrase, or numerical quantity that limits the attribute (subject) of the rule in one way or the other, as defined by the selected Comparison (relationship). The type of attribute selected dictates the type of value that you enter. For example, selecting the Size attribute necessitates the entry of a number as the Value. When you type file extensions, leave off the dot (.) before the extension. Values can include single-byte or multi-byte characters.
AND/OR	Appends an AND or OR operator to the expression, which sets up its relationship to the next expression. Final or single expressions do not require an operator. When you build multiple expressions in a rule, you must use either all AND or all OR expressions. You cannot mix AND and OR operators in the same rule. You must make separate rules for each.
Add	Adds the expression to the List of Expressions.
List of Expressions	Lists the expressions that you have defined for the Content Filtering Rule.
Delete	Deletes the expression that was selected in the List of Expressions.

Action options for content filtering

Table 27 lists the Action options for content filtering.

Table 27 Content filtering Action options

When a violation is detected	Specifies what action to take when Symantec AntiVirus/Filtering for Domino finds a violation of a Content Filtering Rule. ■ No Action: Logs the violation. ■ Copy the document to the Quarantine: Creates a copy in the Symantec AntiVirus/Filtering for Domino Log. ■ Delete the offending attachments: Deletes the attachment whose name, extension, content, or size has violated the Content Filtering Rule. ■ Delete all attachments: Deletes all attachments, even if the rule does not apply to attachments. For example, the rule does not have to specify the document attributes of Attachment name, Attachment ext., or Attachment size for this option to apply. ■ Quarantine the document: Holds the document for administrator review. Open the Log database to process documents with violations. For documents that contain only content violations and no additional virus infections, you can open a report that contains the offending subject line and message content, which helps you determine whether to release the document or adjust the Content Filtering Rule that triggered it. See "About the Quarantine" on page 78. ■ Delete the document: Deletes the document that is in violation of the Content Filtering Rule.

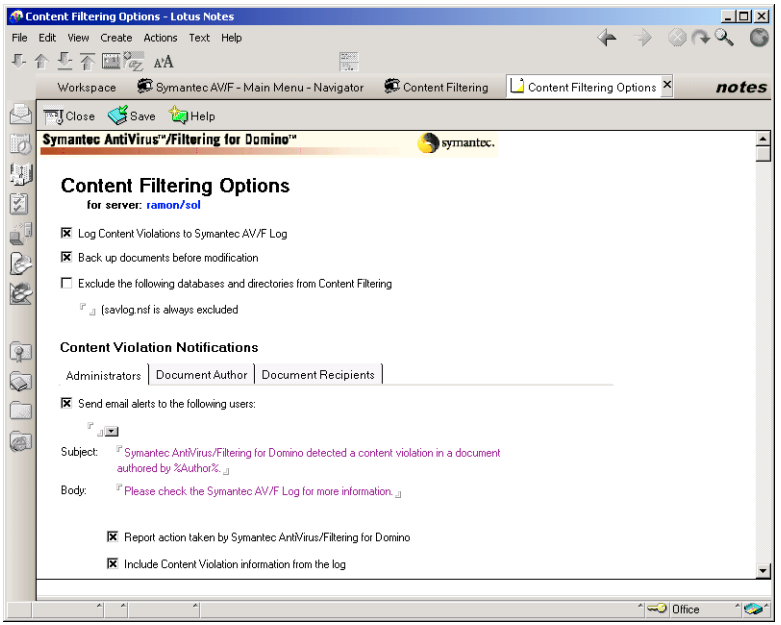
Setting Content Filtering Options

Content Filtering Options apply to all content filtering scanning. They include processing and content filtering violation notifications.

To set Content Filtering Options

1 In the main window, click **Content Filtering**.

2 In the Content Filtering window, click **Content Filter Options.**



3 Check **Log Content Violations to Symantec AV/F Log** if you want to log content violations.

4 Check **Back up document before modification** if you want a copy made in the Symantec AV/F log database before the content violation is processed.

5 Check **Exclude the following databases and directories from Content Filtering**, if desired.

Specify the databases and directories to omit.

6 Specify whom to notify if a content violation is detected.

See "Content Violation Notifications settings" on page 69.

7 On the Action bar, click **Save**.

8 Click **Close**.

Content Violation Notifications settings

Table 28 lists the Content Filtering Notifications options.

Table 28 Content Violation Notifications settings

Administrators	Specifies email alert to send to administrators to advise when a content violation has occurred. Administrators options are as follows: ■ Send email alerts to the following users: Enables the option to send alerts to specified administrators. ■ Custom text to specified administrators: Specifies the subject line and body content of the email message that is sent for the alert that was generated. Use tokens to customize the subject or body of the email alert, as necessary. See "Tokens for customizing email alerts" on page 52. ■ Report action taken by Symantec AntiVirus/Filtering for Domino: Includes the action that was taken by Symantec AntiVirus/Filtering for Domino in the email to the administrator. ■ Include violation information from the log: Includes information about the violation from the Log in the email.
Document Author	Specifies the email alert to send to the author of the infected document. If your policy is to quarantine infected documents, let authors know whom to contact to release the document. If your policy is to delete infected attachments, advise them to scan the source before sending the attachment again. Document Author options are as follows: ■ Send email alerts to document author: Enables the option to send alerts to the document author. ■ Custom text to document author: Specifies the subject line and body content of the email message that is sent for the alert that was generated. Use tokens to customize the subject or body of the email alert as necessary. See "Tokens for customizing email alerts" on page 52. ■ Report action taken by Symantec AntiVirus/Filtering for Domino: Includes the action taken by Symantec AntiVirus/Filtering for Domino in the email to the document author. ■ Include violation information from the log: Includes information about the violation from the Log in the email to the document author.

Document Recipients	Specifies the email alert to send to the intended recipients of the infected document. If your policy is to quarantine infected documents, let users know whom to contact to release the document. If your policy is to delete infected attachments, advise them to contact the document author to resend an uninfected version. Document Recipients options are as follows: ■ Send email alerts to intended recipients: Sends alert to intended recipients of the document. ■ Custom text to intended recipients: Specifies the subject line and body content of the email message that is sent for the alert that was generated. Use tokens to customize the subject or body of the email alert, as necessary. See "Tokens for customizing email alerts" on page 52. ■ Report action taken by Symantec AntiVirus/Filtering for Domino: Includes the action that was taken by Symantec AntiVirus/Filtering for Domino in the email to the recipient. ■ Include violation information from the log: Includes information about the violation from the Log in the email.

Enabling or disabling content filtering

When you create a Content Filtering Rule, Symantec AntiVirus/Filtering for Domino lets you enable or disable that particular rule. You can also enable or disable specific Content Filtering Rules in the listing of rules.

To enable or disable a Content Filtering Rule

1. In the main window, click **Content Filtering**.
2. Select a Content Filtering Rule in the list, then click **Enable** or **Disable**.

Chapter 5

Using the Log

This chapter includes the following topics:

Viewing the Log

The Log/Quarantine database stores server messages, reports of virus incidents or content filtering violations, scan summaries, and predefined statistical reports. In addition to its logging functions, the Log/Quarantine database also hosts the Quarantine and Backup repositories.

See "Managing the Quarantine" on page 77.

See "Managing Backup documents" on page 86.

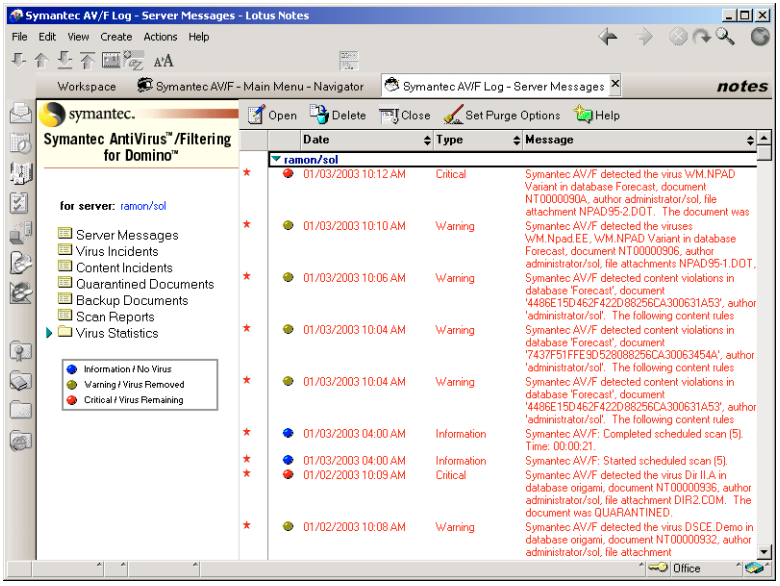
On the Lotus Notes client, you can view these types of data in several views. Symantec AntiVirus/Filtering for Domino lets you view virus and content filtering data separately.

Server messages and incidents are reported with the following severities:

- Information (blue): No violation occurred with the event.
- Warning (green): A violation occurred with the event, but was removed.
- Critical (red): A violation occurred with the event, and remains.

To view the Log

1 In the main window, click **AV/F Log**.



2 Select one of the following Log views:

- Server Messages: Logs server-related events and displays them by Date, Type, and Message. Initially, the Server Messages view sorts by the Date column, but you can click the ascending or descending arrow in the Type or Message column to sort data by that column.
- Virus Incidents: Logs virus detections. Incidents are reported by document, not by database. Symantec AntiVirus/Filtering for Domino uses them to calculate statistics.
- Content Incidents: Displays incidents that were logged because of content filtering violations.
- Quarantined Documents: Lists documents that were quarantined because of viruses or content violations.
- Backup Documents: Lists backups of documents prior to their Symantec AntiVirus/Filtering for Domino repair.
- Scan Reports: Logs summaries of Scheduled Scans and on-demand scans (Scan Now) and displays them by Date, Type, Infected (documents), Cleaned (documents), and Quarantined (documents). Initially, the Scan Reports view sorts by the Date column, but you can click the ascending or descending arrow in another column to sort data by that column.
- Virus Statistics: Displays predefined statistical reports of Log data, sorted in several ways.

3 If you selected Virus Statistics, select one of the following Statistics views:

- Author: Displays cumulative incidents sorted by the Organization & Author column in the Log database with total counts of virus detections or content violations including quarantined and cleaned documents, and virus or content violations for which Symantec AntiVirus/Filtering for Domino sent only a notification.

  Author & Month: Displays the Author view sorted by month.

  Author & Year: Displays the Author view sorted by year.
- Organization: Displays cumulative data from incidents sorted by the Organization & Server database column in the Log database. The view shows the names and total counts of virus detections and content violations. It also shows quarantined and cleaned documents, and virus detections and content violations for which Symantec AntiVirus/Filtering for Domino sent only a notification.

  Org & Month: Displays the Organization view sorted by month.

  Org & Year: Displays the Organization view sorted by year.

- Scan Type: Displays cumulative data from incidents sorted by the Scan Type column in the Log database. The view displays the virus or content filtering violation count and the names of the scan types.

  Scan & Month: Displays the Scan Type view sorted by month.

  Scan & Year: Displays the Scan Type view sorted by year.
- Virus: Displays cumulative virus incidents sorted by the Virus column in the Log database. The view displays the virus names and the count for each.

  Virus & Month: Displays the Virus view sorted by month.

  Virus & Year: Displays the Virus view sorted by month.

The Viruses statistics view counts viruses, not incidents of viruses. For example, if a document contains two viruses, the Viruses statistics view counts each virus separately. Consequently, the totals that are displayed in the Viruses statistics view may not match those displayed in other views.

Managing the Log size

To prevent the Log/Quarantine database from becoming too large, a purge agent runs every night at 1:00 AM when enabled. By default, virus incidents are purged after 365 days. Other Log entries are purged after 30 days.

Note: The purge agent is not replicated. You can only configure it for the master Log database.

Work with the Log purge agent

After granting rights to run restricted agents, you can purge Log items with the purge agent.

To enable the Log purge agent, you must have rights to run unrestricted agents that are set in the Server Document for the Domino Directory (Public Address Book) that belongs to the server.

To grant rights to enable the Log purge agent

1. Open the Domino Directory (names.nsf) for the server.
2. In the left (navigation) pane, open **Server**.
3. Click **Servers**.
4. In the right (view) pane, double-click the server on which Symantec AntiVirus/Filtering for Domino runs.

5 On the Security tab, do one of the following:

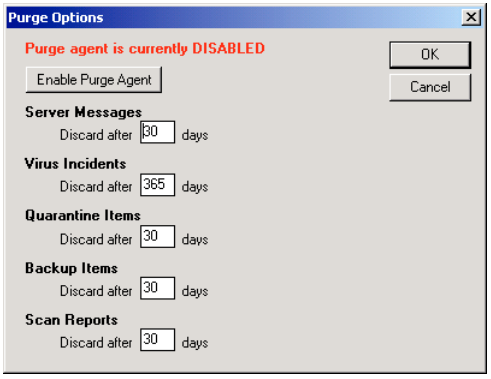
- If you are running Lotus Domino 6.x, under Programmability Restrictions, double-click **Run Simple and Formula Agents** to enter edit mode.
- If you are running Lotus Domino 5.x, under Agent Restrictions, double-click **Run unrestricted LotusScript/Java agents** to enter edit mode.

6 In the box, add the users to whom you want to grant rights for enabling or disabling the Log purge agent.

To purge log items

1 Open the Log database using a Notes ID from a user to whom you have granted rights to disable or enable the Log purge agent.

2 On the Action bar, click **Set Purge Options**.



3 In the Purge Options dialog box, type the following:

- Under Server Messages, the number of days to wait to purge server messages
- Under Virus Incidents, the number of days to wait to purge all virus incidents
- Under Scan Reports, the number of days to wait to purge all scan reports

After Symantec AntiVirus/Filtering for Domino purges the items, it waits for the specified number of days before purging the next batch of items.

4 Click **Enable Purge Agent**.

5 In the Choose Server To Run On dialog box, select the server on which the agent is to run, then click **OK**.

6 Click **OK** to close the dialog box.

Chapter 6

Managing the Quarantine

This chapter includes the following topics:

About the Quarantine

If you have configured it to do so, Symantec AntiVirus/Filtering for Domino can isolate scanned documents that it has found to be suspicious in the Log/Quarantine database.

When an email is quarantined, Symantec AntiVirus/Filtering for Domino places the entire email message and any attachments in the Quarantine, regardless of which part of the document is infected or has offending content. It does not forward any part of the email. Symantec AntiVirus/Filtering for Domino can also quarantine infected Lotus Notes database documents.

The Quarantine stores two types of documents: Quarantined and Backup documents. Symantec AntiVirus/Filtering for Domino displays Quarantined documents separately from Backup documents.

All views show when the document was quarantined, which database was affected, who authored the document, and which virus detection or content violation rule was involved. The views also show whether the document has been released, that is, restored to its original database to complete processing as originally planned.

Quarantined documents

Quarantined documents are infected documents that have not been repaired or documents with content violations.

While suspicious documents are in Quarantine, administrators can manage them by reviewing and taking action on them as permitted. Actions include deleting the document or attachment, saving the attachment or adding a new one, and releasing the document. Quarantined infected documents must be repaired (or their infected attachments deleted) before they can be released. For a document with a content violation, you can edit the document in the Quarantine to remove the violation and then release it.

Backup documents

As a data safety precaution, administrators can configure Symantec AntiVirus/Filtering for Domino (from Group Options) to store a backup copy of any document that contains content violations or infected attachments. That way a copy is available if anything happens to the original.

How documents get quarantined

Symantec AntiVirus/Filtering for Domino quarantines documents only when the following occurs:

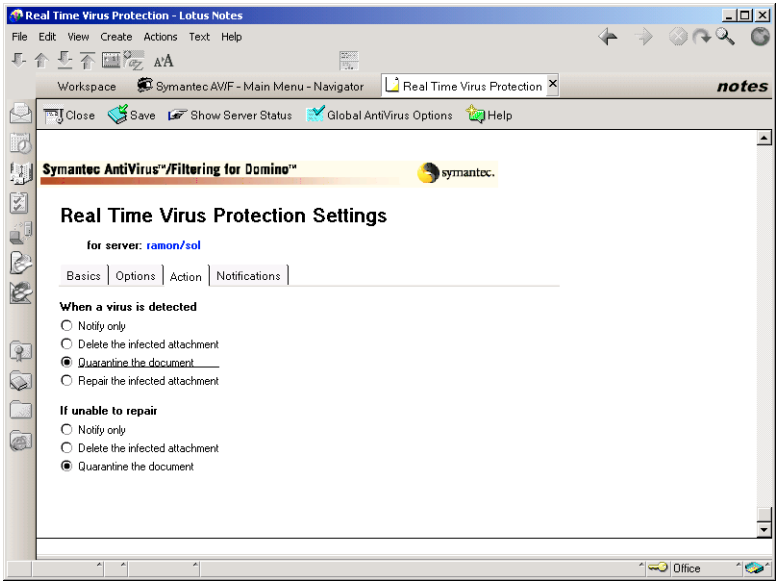
- Content filtering is configured to quarantine or copy documents when a content violation has occurred in an email message or attachment (as specified by the Content Filtering Rule).
- Real Time scanning, Scan Now scans, or Scheduled Scans are configured to quarantine documents after a virus is detected.
- Real Time scanning, Scan Now scans, or Scheduled Scans are configured to repair infected attachments, but quarantine any documents that have attachments that cannot be repaired.

The option that holds content violations or infected documents in Quarantine is Quarantine the document. It's located on the Action tab of the Scan Now, Real Time, Scheduled Scan, or Content Filtering forms.

On those same tabs, the options that quarantine documents that have attachments that cannot be repaired are Repair the infected attachment (under If a virus is detected), and Quarantine the document (under If unable to repair).

Figure I shows the Action tab of Real Time scanning.

Figure I Action options for scans (Real Time shown)



Managing Quarantined documents

Before you can release an infected item from the Quarantine, you must ensure that it no longer contains infected attachments or attachments that violate Content Filtering Rules. You can save, delete, or replace attachments of quarantined items.

Actions to take on Quarantined documents

You can take actions on an infected document, attachment, or content violation in any of the following ways:

- Save Attachments: Saves a copy of the attachment or attachments to a location that you choose. Saving quarantined attachments provides the same safety measure as placing them in the Backup Documents view. However, you may not have configured the scan that quarantined the item to also isolate a copy of the quarantined document to the Backup Documents database. This option gives you another chance to save a copy.

  After you save a copy, you may want to run another scan to repair it (perhaps using updated virus definitions). Once the attachment is repaired, you can add it to the Quarantine Document again and release it to its intended recipient.

  If the attachment contains a content violation, you may want to save it to a location where someone else can review it before deciding what further action to take.

- Add Attachment: Adds the file that you select to the quarantined document. Before releasing a document from the Quarantine, you can add a newly repaired compressed file, replace an infected file with a known good copy, or add a procedural file with instructions to scan a workstation.

- Delete Attachments: Removes the attachments and prompts you before deleting each one. When you delete attachments, the quarantined item remains in the Quarantine view without the attachments.

- Release: Releases the document from the Quarantine and restores it to its original database. When you release a document, Symantec AntiVirus/Filtering for Domino changes the Restored field from No to the date and time of the restore in the Quarantine view. The quarantined item remains in the Quarantine until Symantec AntiVirus/Filtering for Domino purges it or you select it and then click Delete on the Action bar to delete it from the view.

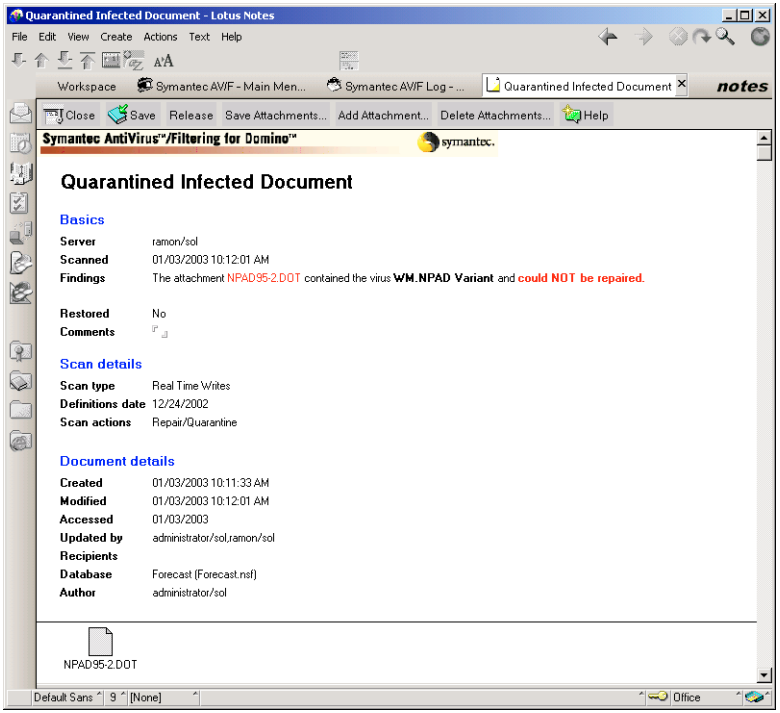
Managing infected documents

You can manage infected documents from the Content Incidents, Quarantined Documents, or Backup Documents views. You can delete and replace attachments, which lets you repair them, for example, with LiveUpdate.

To manage infected documents

1. In the main window, click **AV/F Log**.
2. In the left pane, click **Quarantined Documents**.
3. To delete a document from the database, in the right pane, click the item, then on the Action bar, click **Delete**.

   You are prompted to delete the document from the database. After deleting, press **F9** to refresh the view.
4. To view the Quarantined Document report, in the right pane, double-click an item with a virus infection.



5 On the Action bar, select one of the following:

- Save Attachments**:** You are prompted to save the attachment as a file in a location that you select.
- Add Attachment: You are prompted to type the path of the file to add. After it is added, press **F9** to refresh the view.
- Delete Attachments: You are prompted on each attachment before the deletion takes place. After they are deleted, press **F9** to refresh the view.

6 To release a quarantined document, on the Action bar, click **Release**.

You are prompted to continue, which restores the quarantined document to its original database.

If the document is still infected, it will be detected and quarantined again.

7 On the Action bar, click **Close**.

You are prompted to save your changes.

Released items remain in the Quarantine list until Symantec AntiVirus/Filtering for Domino purges them or you select them individually and click Delete to manually remove them.

Releasing repaired infected documents

Some documents require careful review before you decide what to do with them, while you can release others immediately. After making sure that the document or email no longer contains infected attachments, you can release quarantined documents.

You can routinely purge quarantined documents from the Quarantine and Backup Document views.

See "Managing the Quarantine database size" on page 85.

See "Managing Backup documents" on page 86.

If you release a document that still has infected attachments, Symantec AntiVirus/Filtering for Domino quarantines it again.

To release repaired infected documents from the Quarantine

1 In the main window, click **AV/F Log**.

2 In the left pane, click **Quarantined Documents**.

3 To release a document without viewing it, in the right pane, select the document, then on the Action bar, click **Release from Quarantine**.

You are prompted to confirm the release.

4 To view a document before releasing it, in the right pane, double-click an item.

5 As an option in the Quarantined Document view, in the Comments field, you can type a note describing the status of the item.

6 On the Action bar, click **Release**.

You are prompted to continue, which restores the Quarantined document to its original database.

To delete the Quarantined Document from the view, on the Action bar, click **Delete**.

7 On the Action bar, click **Close**.

You are prompted to save your changes.

Managing documents with content violations

You can manage quarantined documents with content violations in the Quarantined Documents view. You can delete attachments in the quarantined item, add attachments to it, or save attachments to other locations so that others can review them. In addition, you can edit the document to remove the content violation and then release the document.

To manage documents with content violations

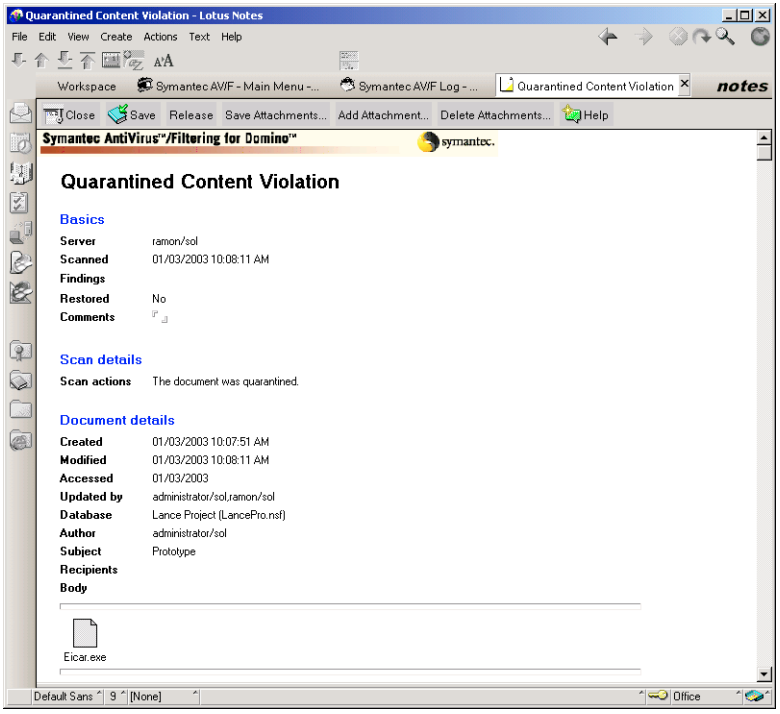
1 In the main window, click **AV/F Log**.

2 In the left pane, click **Quarantined Documents.**

3 To delete a document from the database, in the right pane, select the item, then on the Action bar, click **Delete**.

You are prompted to delete the document from the database. After you delete it, press **F9** to refresh the view.

4 To view the Quarantined Content Violation, in the right pane, double-click an item with a content violation.



5 On the Action bar, you can select one of the following:

- Save Attachments: You are prompted to save the attachment as a file in a location that you select.
- Add Attachment: You are prompted to type the path of the file to add. After it is added, press **F9** to refresh the view.
- Delete Attachments: You are prompted on each attachment before the deletion takes place. After it is deleted, press **F9** to refresh the view.
- Release: The document is released from the Quarantine and restored to its original database. You can edit the document to remove the content violation. When you release a document, Symantec AntiVirus/Filtering for Domino changes the Restored field from No to the date and time of the restore in the Quarantine view.

6 Optionally, in the Quarantined Content Violation view, in the Comments field, type a note that describes the status of the item.

7 On the Action bar, click **Close**.

Managing the Quarantine database size

To prevent the Quarantine database from becoming too large, a purge agent runs every night at 1:00 AM when enabled. By default, Symantec AntiVirus/Filtering for Domino purges entries after 30 days. However, you can routinely purge quarantined documents from the Quarantine and Backup document views.

Note: The purge agent is not replicated. You can only configure it for the master Quarantine database.

To enable the Quarantine purge agent, you must grant rights to run unrestricted agents in the Server Document for the Domino Directory (Public Address Book) that belongs to the server.

Work with the Quarantine purge agent

After granting rights to run restricted agents, you can purge Quarantined documents with the purge agent.

To grant rights to enable the Quarantine purge agent

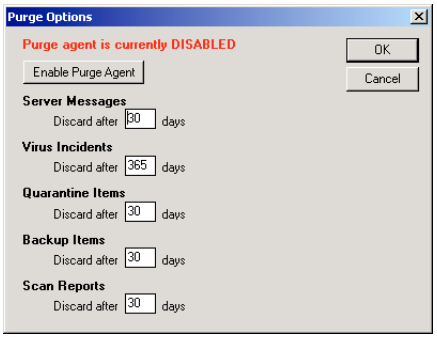
1. Open the Domino Directory (names.nsf) for the server.
2. In the left (navigation) pane, open **Server**.
3. Click **Servers**.
4. In the right (view) pane, double-click the server on which Symantec AntiVirus/Filtering for Domino runs.
5. On the Security tab, do one of the following:
   - If you are running Lotus Domino 6.x, under Programmability Restrictions, double-click **Run Simple and Formula Agents** to enter edit mode.
   - If you are running Lotus Domino 5.x, under Agent Restrictions, double-click **Run unrestricted LotusScript/Java agents** to enter edit mode.
6. In the box, add the users to whom you want to grant rights to enable or disable the Quarantine purge agent.

To purge quarantined documents

1. Open the Quarantine database using a Notes ID from a user to whom you have granted rights to disable or enable the Quarantine purge agent.

2 In the left pane, click **Quarantined Documents** to display a view of quarantined items in the right pane.

3 On the Action bar, click **Set Purge Options**.



4 In the Purge Options dialog box, type the following:

- Under Quarantine Items, the number of days to wait to purge virus infection and content violation items in the Quarantine view
- Under Backup Items, the number of days to wait to purge virus infection and content violation items in the Backup Documents view

After Symantec AntiVirus/Filtering for Domino purges the items, it waits for the specified number of days before purging the next batch of items.

5 Click **Enable Purge Agent**.

6 In the Choose Server To Run On dialog box, select the server on which the agent is to run, then click **OK**.

7 Click **OK** to close the dialog box.

Managing Backup documents

You can configure Symantec AntiVirus/Filtering for Domino to make a backup copy of infected documents before they are repaired or deleted in the Quarantine database. (The option to back up documents is on the Backup tab of Group Options.)

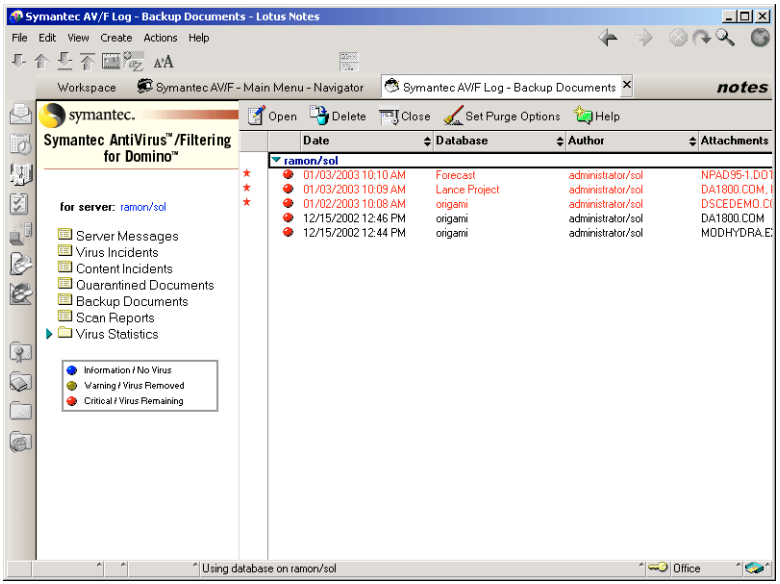
The Backup Documents view shows when the item was backed up, which database was involved, who the author was, and the name of the infected document, email, or email attachment.

You can manage the Backup Documents view in much the same way as the Quarantine Document list, except that you cannot add or delete attachments, or release documents to their original databases.

To manage Backup documents

1 In the main window, click **AV/F Log**.

2 In the left pane, click **Backup Documents**.



3 To delete an item in the right pane, select it, then click **Delete** to mark it for deletion.

When you close the view, you are prompted to delete the item from the database.

4 To review a backup document, double-click it to open it.

5 To save the backup attachment to another location, open it, then click **Save Attachments**.

You are prompted to save the attachment as a file in a location that you select.

Chapter 7

Maintaining current protection

This chapter includes the following topics:

About LiveUpdate

Symantec AntiVirus/Filtering for Domino relies on up-to-date information to detect and eliminate viruses. One of the most common reasons you may have a virus problem is that you have not updated your protection files since you installed the product. Symantec regularly supplies updated virus definitions files, which contain information about all newly discovered viruses.

With LiveUpdate, Symantec AntiVirus/Filtering for Domino connects automatically to Symantec sites and determines if your virus definitions need updating. If so, it downloads the proper files and installs them in the proper location.

If you do not want to permit direct access to the Internet from your Lotus Domino servers or you are running proxy servers, you can set up an internal LiveUpdate server with LiveUpdate Administrator and configure Symantec AntiVirus/Filtering for Domino to access the internal LiveUpdate server instead.

See "Configuring an internal LiveUpdate server" on page 91.

How to update virus protection

LiveUpdate connects over the Internet to a site that Symantec maintains for LiveUpdate use. Generally, you do not have to do anything to configure LiveUpdate. The only requirement is an Internet connection.

To immediately update virus definitions

1. In the main window, click **LiveUpdate**.
2. On the Action bar, click **Run LiveUpdate Now**.

To schedule automatic LiveUpdate

1. In the main window, click **LiveUpdate**.
2. Under Schedule, check **Enable LiveUpdate**.
3. To replicate the virus definitions database to other Domino servers, check **Save downloaded virus definitions in the Symantec AV/F definitions database**.

   Don't check this option if you have Symantec AntiVirus/Filtering for Domino installed on a single Domino server or do not plan to replicate the definitions database.

4 Type the time of day that LiveUpdate runs and select the frequency.
Specify an off-peak time for high-traffic networks.

5 On the Action bar, click **Save**, then click **Close**.

Configuring an internal LiveUpdate server

LiveUpdate operation is controlled by settings in the /etc/liveupdate.conf file. By default, an HTTP connection is made to the Symantec server. You can change the settings to point to an internal LiveUpdate server using either an FTP or HTTP protocol connection. The LiveUpdate server is created using the separately supplied and installed LiveUpdate Administration Utility.

To configure Symantec AntiVirus/Filtering for Domino to use an internal LiveUpdate server via FTP

1 For safety, make a backup copy of the following file:
/etc/liveupdate.conf

2 Make the following changes to the liveupdate.conf file:

- Change the protocol= line to protocol= ftp for an FTP connection.
- Change the host= line from liveupdate.symantec.com to your internal LiveUpdate server.
- Change the login= and password= settings to the login and password for your FTP server.

Do not make changes to any other lines in the file.

To configure Symantec AntiVirus/Filtering for Domino to use an internal LiveUpdate server via HTTP

1 For safety, make a backup copy of the following file:
/etc/liveupdate.conf

2 Make the following changes to the liveupdate.conf file:

- Change the protocol setting to protocol=http.
- Change the host= line from liveupdate.symantec.com to your internal LiveUpdate server.

Do not make changes to any other lines in the file.

You can configure liveupdate.conf to use a host (.hst) file created by the LiveUpdate Administration Utility (LUAdmin), which is a separately supplied program that runs on Windows NT.

For more information, see the LiveUpdate Administration Utility document (luadmin.pdf) supplied with the LiveUpdate Administration Utility to configure the .hst file for use with Symantec AntiVirus/Filtering for Domino.

If you want to continue using an existing liveupdt.hst file from an earlier installation, make the following modification instead.

To use an existing liveupdt.hst file

- Add the following line to the /etc/liveupdate.conf file:

  hostfile=<full path to the .hst file on the server>

  If the hostfile= parameter is included in liveupdate.conf, all other lines are ignored and data from the .hst file is used instead.

To create a new liveupdt.hst file

- Use the separately supplied LiveUpdate Administration Utility (LUAdmin), which runs under Windows.

Index

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W